

Summer 1967

# SOME TYPES OF UNIQUE FACTORIZATION IN INTEGRAL DOMAINS

RAYMOND A. BEAUREGARD

Follow this and additional works at: <https://scholars.unh.edu/dissertation>

---

## Recommended Citation

BEAUREGARD, RAYMOND A., "SOME TYPES OF UNIQUE FACTORIZATION IN INTEGRAL DOMAINS" (1967). *Doctoral Dissertations*. 874.  
<https://scholars.unh.edu/dissertation/874>

This Dissertation is brought to you for free and open access by the Student Scholarship at University of New Hampshire Scholars' Repository. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of University of New Hampshire Scholars' Repository. For more information, please contact [nicole.hentz@unh.edu](mailto:nicole.hentz@unh.edu).

**This dissertation has been  
microfilmed exactly as received**

**69-759**

**BEAUREGARD, Raymond A, 1943-  
SOME TYPES OF UNIQUE FACTORIZATION IN  
INTEGRAL DOMAINS.**

**University of New Hampshire, Ph.D., 1968  
Mathematics**

**University Microfilms, Inc., Ann Arbor, Michigan**

SEVERAL TYPES OF UNIQUE FACTORIZATION IN INTEGRAL DOMAINS

by

RAYMOND A. BEAUREGARD

M.S., University of New Hampshire, 1966

A THESIS

Submitted to the University of New Hampshire

In Partial Fulfillment of

The Requirements for the Degree of

Doctor of Philosophy

Graduate School

Department of Mathematics

August, 1968

This thesis has been examined and approved.

Richard E. Johnson  
Thesis director, Richard E. Johnson, Prof. of Mathematics

H. Evans Munroe  
H. Evans Munroe, Chairman and Prof. of Mathematics

Edward H. Batho  
Edward H. Batho, Prof. of Mathematics

Homer F. Bechtell  
Homer F. Bechtell, Asso. Prof. of Mathematics

David M. Burton  
David M. Burton, Asso. Prof. of Mathematics

18 June 1968  
Date

## TABLE OF CONTENTS

ABSTRACT	iv
INTRODUCTION	1
I. PRELIMINARIES	6
II. RIGHT QUOTIENT MONOIDS	14
2.1 Definition and consequences	14
2.2 Unique factorization	21
III. APPLICATION TO ARBITRARY ELEMENTS IN A PRI DOMAIN	25
3.1 Unique factorization and infinite primes	25
3.2 The local case	31
3.3 Example: skew polynomial extensions	35
3.4 An example in the non-Bezout case	41
IV. APPLICATION TO FINITE DIMENSIONAL ELEMENTS IN A RIGHT BEZOUT DOMAIN	45
4.1 Unique factorization and similar primes	45
4.2 Example	49
BIBLIOGRAPHY	53

# ABSTRACT

## SOME TYPES OF UNIQUE FACTORIZATION IN INTEGRAL DOMAINS

by

RAYMOND A. BEAUREGARD

In the present paper we obtain some general results concerning unique factorization with respect to right quotient monoids in a weak Bezout domain  $R$  satisfying the ascending chain condition for principal right ideals. These results in turn are used to describe some types of unique factorization that occur in  $R$ .

A subset  $S$  of an integral domain  $R$  is called a right quotient monoid in  $R$  if it is a submonoid of the multiplicative monoid of non-zero elements of  $R$  and satisfies certain right quotient conditions. If in addition  $R$  is a weak Bezout domain satisfying the ascending chain condition for principal right ideals, we prove that each non-zero element  $z$  of  $R$  can be factored in the form  $z = rs$  where  $s \in S$  and  $r$  has no non-unit right factor in  $S$ . This factorization is unique in the sense that any other such factorization must have the form  $z = (ru)(u^{-1}s)$  where  $u$  is a unit in  $R$ . A collection of right quotient monoids  $\{S_\alpha \mid \alpha \in I\}$  indexed by an initial segment of ordinals  $I$  is called a right quotient chain in an integral domain  $R$  if  $\bigcup_{\beta < \alpha} S_\beta = S_\alpha$  if  $\alpha$  is a limit ordinal in  $I$  and  $S_\beta \subsetneq S_\alpha$  if  $\beta < \alpha$ ,  $\beta, \alpha \in I$ . If in addition  $R$  is a weak Bezout domain satisfying the ascending chain condition for principal right ideals then we are able to prove the following. Each non-zero element  $z$  of  $R$  can be written as  $z = sa_{\alpha_1} \dots a_{\alpha_n}$  where  $\alpha_i$  are non-limit ordinals such that  $\alpha_1 > \dots > \alpha_n$ ,  $a_{\alpha_i} \in S_{\alpha_i}$ ,  $a_{\alpha_i}$  has no non-unit right factor in  $S_{\alpha_i-1}$  ( $S_{-1}$  denotes the

group of units of  $R$ ), and  $s$  has no non-unit right factor in  $\bigcup_{\alpha \in I} S_\alpha$ . The factorization is unique in the sense that if  $z = r b_{\beta_1} \dots b_{\beta_n}$  is another such factorization, then  $n = m$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, n$ ), and there are units  $u_0, u_1, \dots, u_{n-1}$  in  $R$  such that  $s = r u_0$ ,  $a_{\alpha_n} = u_{n-1}^{-1} b_{\alpha_n}$ , and  $a_{\alpha_i} = u_{i-1}^{-1} b_{\alpha_i} u_i$  ( $i \neq 0, n$ ).

One application of the preceding results deals with unique factorization of all of the non-zero elements of a PRI domain  $R$ .  $\text{Inf}^{(\alpha)}$  primes are defined for each non-limit ordinal  $\alpha$ .  $\text{Inf}^{(0)}$  primes are the usual primes, and  $\text{inf}^{(\alpha)}$  primes have infinite dimension if  $\alpha \neq 0$ . We prove that each non-zero element  $a$  of  $R$  can be factored as  $a = z_{\alpha_1} \dots z_{\alpha_n}$  where  $z_{\alpha_i}$  is a uniquely determined product of  $\text{inf}^{(\alpha_i)}$  primes ( $i = 1, 2, \dots, n$ ). The factorization is unique in the sense that if  $a = y_{\beta_1} \dots y_{\beta_m}$  is another such factorization then  $n = m$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, n$ ), and there are units  $u_1, \dots, u_{n-1}$  in  $R$  such that  $z_{\alpha_1} = y_{\alpha_1} u_1$ ,  $z_{\alpha_n} = u_{n-1}^{-1} y_{\alpha_n}$ , and  $z_{\alpha_i} = u_{i-1}^{-1} y_{\alpha_i} u_i$  ( $i \neq 1, n$ ).

Another application of the general results deals with the set  $R'$  of finite dimensional elements in a right Bezout domain  $R$ . An element in  $R'$  is called  $p$ -primary ( $p$  a prime) if it is a product of primes that are similar to  $p$ . That the members of  $R'$  can be factored into primary elements follows easily. Under certain conditions we are able to prove that the primary factorization is unique in two different respects. In one case if an element  $z$  in  $R'$  can be given two primary factorizations  $z = a_{p_1} \dots a_{p_n} = b_{p_1} \dots b_{p_n}$  where  $a_{p_i}$  and  $b_{p_i}$  are  $p_i$ -primary such that  $p_i \not\sim p_j$  if  $i \neq j$ , then there are units  $u_1, \dots, u_{n-1}$  in  $R$  such that  $a_{p_1} = b_{p_1} u_1$ ,  $a_{p_n} = u_{n-1}^{-1} b_{p_n}$ , and  $a_{p_i} = u_{i-1}^{-1} b_{p_i} u_i$  ( $i \neq 1, n$ ). In the other case we assume that some non-unit element  $z$  of  $R'$  can be given a primary factorization  $z = a_{p_1} \dots a_{p_n}$  where  $a_{p_i}$  are  $p_i$ -primary such that  $p_i \not\sim p_j$

if  $i \neq j$ . We prove that if  $z = b_{q_1} \dots b_{q_m}$  is another factorization of  $z$  into  $q_i$ -primary elements  $b_{q_i}$  such that  $q_i \not\sim q_j$  if  $i \neq j$ , then there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $b_{q_i} \sim b_{q_{\pi(i)}}$  ( $i = 1, 2, \dots, n$ ). (The symbol  $\sim$  denotes similarity).

Throughout the paper several examples are discussed in detail in order to illustrate the theory and indicate the necessity of some of the hypotheses. Included in one of the examples is A. V. Jategaonkar's recent theory of skew polynomial extensions by which it is possible to construct PRI domains with  $\text{inf}^{(\alpha)}$  primes where  $\alpha$  is any initially given ordinal that is not a limit ordinal.



## INTRODUCTION

In the present paper we obtain some general results concerning unique factorization with respect to right quotient monoids in a weak Bezout domain  $R$  satisfying the ascending chain condition for principal right ideals. These results in turn are used to describe some types of unique factorization that occur in  $R$ .

The known types of unique factorization that occur in a weak Bezout domain  $R$  deal with the set of elements  $R'$  of  $R$  that have finite dimension. For example it is well known (Theorem 1) that each member  $z$  of  $R'$  can be factored into primes:  $z = p_1 \dots p_n$ , and if  $z = q_1 \dots q_m$  is another such factorization, then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $p_i$  and  $q_{\pi(i)}$  are similar ( $i = 1, 2, \dots, n$ ). For a PRI domain  $R$  another type of unique factorization for the members of  $R'$  is described by A. B. Johnson in [9]. An element  $a \in R'$  is called simple if  $[aR, R]$  has the property that  $[aR, R] = [aR, B] \cup [B, R]$  implies  $B = aR$  or  $B = R$ . Johnson proves that each element  $z$  of  $R'$  can be factored into simple elements  $z = a_1 \dots a_n$  such that no subproduct  $a_i \dots a_j$ ,  $i < j$ , of  $z$  is simple. Any other factorization of  $z$  into simple elements of this type must have the form  $z = (a_1 u_1)(u_1^{-1} a_2 u_2) \dots (u_{n-1}^{-1} a_n)$ , where  $u_1, \dots, u_{n-1}$  are units in  $R$ .

We describe two additional types of unique factorization. The first concerns all of the non-zero elements of a PRI domain  $R$ , and the second deals with the members of  $R'$  in a right Bezout domain  $R$ . Both are obtained by applying more general results concerning unique factorization with respect to right quotient monoids.

A subset  $S$  of an integral domain  $R$  is called a right quotient

monoid if it is a submonoid of the multiplicative monoid of non-zero elements of  $R$  and satisfies certain right quotient conditions. If  $R$  is a weak Bezout domain satisfying the ascending chain condition for principal right ideals we prove (Factorization lemma) that each non-zero element  $z$  of  $R$  can be uniquely written in the form  $z = rs$  where  $s \in S$  and  $r$  has no non-unit right factor in  $S$ . This factorization is unique in the sense that any other such factorization must have the form  $z = (ru)(u^{-1}s)$ , where  $u$  is a unit in  $R$ . A set of right quotient monoids  $\{S_\alpha \mid \alpha \in I\}$  indexed by an initial segment of ordinals  $I$  is called a right quotient chain in an integral domain  $R$  if  $\bigcup_{\beta < \alpha} S_\beta = S_\alpha$  if  $\alpha$  is a limit ordinal in  $I$  and  $S_\beta \subsetneq S_\alpha$  if  $\beta < \alpha$ ,  $\beta, \alpha \in I$ . If  $R$  is a weak Bezout domain satisfying the ascending chain condition for principal right ideals then we are able to prove the following. Each non-zero element  $z$  of  $R$  can be written as  $z = sa_{\alpha_1} \dots a_{\alpha_n}$  where  $\alpha_i$  are non-limit ordinals such that  $\alpha_1 > \dots > \alpha_n$ ,  $a_{\alpha_i} \in S_{\alpha_i}$ ,  $a_{\alpha_i}$  has no non-unit right factor in  $S_{\alpha_i-1}$  ( $S_{-1}$  denotes the group of units of  $R$ ), and  $s$  has no non-unit right factor in  $\bigcup_{\alpha \in I} S_\alpha$ . The factorization is unique in the sense that if  $z = rb_{\beta_1} \dots b_{\beta_m}$  is another such factorization, then  $n = m$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, n$ ), and there are units  $u_0, u_1, \dots, u_{n-1}$  in  $R$  such that  $s = ru_0$ ,  $a_{\alpha_n} = u_{n-1}^{-1} b_{\alpha_n}$ , and  $a_{\alpha_i} = u_{i-1}^{-1} b_{\alpha_i} u_i$  ( $i \neq 0, n$ ).

Our first application of the preceding results deals with unique factorization of all of the non-zero elements of a PRI domain  $R$ .  $\text{Inf}^{(\alpha)}$  primes are defined for each non-limit ordinal  $\alpha$ .  $\text{Inf}^{(0)}$  primes are the usual primes, and  $\text{inf}^{(\alpha)}$  primes have infinite dimension if  $\alpha \neq 0$ . We prove (Theorem 5) that each non-zero element  $a$  of  $R$  can be factored as  $a = z_{\alpha_1} \dots z_{\alpha_n}$  where  $z_{\alpha_i}$  is a uniquely determined product of  $\text{inf}^{(\alpha_i)}$  primes ( $i = 1, 2, \dots, n$ ). The factorization is unique in

the sense that if  $c = y_{\beta_1} \dots y_{\beta_m}$  is another such factorization then  $n = m$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, n$ ), and there are units  $u_1, \dots, u_{n-1}$  in  $R$  such that  $z_{\alpha_1} = y_{\alpha_1} u_1$ ,  $z_{\alpha_n} = u_{n-1}^{-1} y_{\alpha_n}$ , and  $z_{\alpha_i} = u_{i-1}^{-1} y_{\alpha_i} u_i$  ( $i \neq 1, n$ ).

The second application of the general results deals with the set of elements  $R'$  in a right Bezout domain  $R$ . An element is called  $p$ -primary ( $p$  a prime) if it is a product of primes that are similar to  $p$ . Since a number  $z$  of  $R'$  is a product of primes, say  $p_i$ , then  $z$  is the product of  $p_i$ -primary elements. Under certain conditions we are able to prove that the primary factorization is unique in two different respects. In one case (Theorem 9) if  $z = a_{p_1} \dots a_{p_n} = b_{p_1} \dots b_{p_n}$  are two factorizations of  $z$  into  $p_i$ -primary elements  $a_{p_i}, b_{p_i}$  such that  $p_i \not\sim p_j$  if  $i \neq j$ , then there are units  $u_1, \dots, u_{n-1}$  in  $R$  such that  $a_{p_1} = b_{p_1} u_1$ ,  $a_{p_n} = u_{n-1}^{-1} b_{p_n}$ , and  $a_{p_i} = u_{i-1}^{-1} b_{p_i} u_i$  ( $i \neq 1, n$ ). In the other case (Theorem 10) we assume that some non-unit element  $z$  of  $R'$  can be given a primary factorization  $z = a_{p_1} \dots a_{p_n}$  where  $a_{p_i}$  are  $p_i$ -primary and  $p_i \not\sim p_j$  if  $i \neq j$ . We prove that if  $z = b_{q_1} \dots b_{q_m}$  is another factorization of  $z$  into  $q_i$ -primary elements  $b_{q_i}$  such that  $p_i \not\sim p_j$  if  $i \neq j$ , then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that

$$a_{p_i} \sim b_{q_{\pi(i)}} \quad (i = 1, 2, \dots, n). \quad (\text{The symbol } \sim \text{ denotes similarity}).$$

The present paper is self contained and is divided into four chapters. The first chapter contains preliminary definitions and well known results. The definition of Bezout domains and Theorem 1 concerning unique prime factorization for weak Bezout domains are due to P. M. Cohn [2]. Theorem 2 which generalizes Theorem 1 for weak Bezout domains appears to be new.

In Chapter 2 we define right quotient monoids in an integral domain  $R$ . If  $S$  is a right quotient monoid in  $R$ , then it is possible to

form a right quotient ring  $K = RS^{-1}$ . The ring  $K$  is an integral domain containing  $R$  with the property that the set of units of  $K$  that belong to  $R$  is precisely  $S$ . In Section 2.1 we prove a number of lemmas concerning  $R$  and  $K$ . In particular we determine those properties which when possessed by  $R$  are also possessed by  $K$ . We also describe (Theorem 4) the relationship between the lattices of right ideals of  $R$  and  $K$  respectively. In Section 2.2 we prove two key results concerning unique factorization in a weak Bezout domain  $R$  satisfying the ascending chain condition for principal right ideals. The Factorization lemma deals with unique factorization with respect to a right quotient monoid. This result is used repeatedly in Chapter 4 to obtain the theorems concerning the primary factorization. We also use the Factorization lemma to prove the Factorization theorem which deals with unique factorization with respect to a right quotient chain.

In Chapter 3, Section 3.1, we apply the Factorization theorem to a particular chain of right quotient monoids that exists in a PRI domain  $R$ . Theorem 5 concerning unique factorization into products of infinite primes results. In Section 3.2 we obtain some special results for the local case. In particular we determine conditions under which a PRI domain is also a PLI domain (Theorems 6 and 7 and the corollaries). In section 3.3 we illustrate Theorem 5 with an example. If such an example is to be non-trivial it must be a PRI domain containing elements of infinite dimension. Until recently few such rings were known. However they do occur, for example, in [5, p.598]. The example that we describe in Section 3.3 deals with A. V. Jategaonkar's recent theory of skew polynomial extensions [3]. Using his methods it is possible to construct a PRI domain containing  $\text{inf}^{(\alpha)}$  primes where  $\alpha$  is an initially given

ordinal that is not a limit ordinal. Theorem 8 is a restatement of Theorem 5 for this special case. In Section 3.4 we give an example of a non-Bézout domain to illustrate how some of the desirable properties may fail to hold in that case.

Another application of the results of Section 2.2 is made in Chapter 4. In Section 4.1 we use the Factorization lemma to describe two kinds of uniqueness that can occur in the primary decomposition of the elements of finite dimension in a right Bézout domain (Theorems 9 and 10). In Section 4.2 we give an example to illustrate the necessity of some of the hypotheses.

It is a pleasure for the author to express appreciation and gratitude to Professor R. B. Johnson for his encouragement and guidance in the development of the present work.

## CHAPTER 1

## PRELIMINARIES

Throughout this thesis we assume that all rings are integral domains with unity. An integral domain in which every right ideal is a principal right ideal is called a PRI domain. A PLI domain is defined similarly. The classical example of a PRI domain is the ring of skew polynomials  $R[x, \sigma] = \{ \sum x^i a_i \mid a_i \in R \}$  over a skew field  $R$ , where  $\sigma$  is an endomorphism on  $R$  and multiplication is determined by the commutation rule  $ax = xa^\sigma$ ,  $a \in R$ . Thus if  $f = a_0 + xa_1 + \dots + x^n a_n$  and  $g = b_0 + xb_1 + \dots + x^m b_m$  ( $a_i, b_i \in R$ ), then the product of  $f$  and  $g$  is given by  $fg = a_0 b_0 + x(a_0^\sigma b_1 + a_1 b_0) + \dots + x^{n+m} (\sigma^n a_n) b_m$  ( $\sigma^n$  denotes the composition of  $\sigma$  with itself  $n$  times). Addition of polynomials is the usual pointwise addition. This ring was first described by Ore [10].

An integral domain  $R$  in which the sum and intersection of any two principal right ideals is again a principal right ideal is called a right Bezout domain. Thus  $R$  is a right Bezout domain iff the set of principal right ideals is a sub-lattice of the lattice of all right ideals of  $R$ . Similar remarks hold for left Bezout domains.

The condition that  $R$  be a right Bezout domain can be weakened by requiring that the sum and intersection of any two principal right ideals is again a principal right ideal if the intersection is non-zero. In this case  $R$  is called a (right) weak Bezout domain. (Left) weak Bezout domains are defined similarly. However it can be shown (see Cohn [3]) that the weak Bezout condition is left-right symmetric, i.e.,  $R$  is a (right) weak Bezout domain iff  $R$  is a (left) weak Bezout domain. Therefore the adjective right or left is usually omitted and

one speaks of weak Bezout domains.

Let  $R$  be an integral domain. Two elements  $a, \bar{a} \in R$  are called similar (written  $a \sim \bar{a}$  or  $a \sim_R \bar{a}$ ) if  $R/aR \cong R/\bar{a}R$  as right  $R$ -modules. It can be shown that this definition is left-right symmetric. In addition similarity can be characterized as follows:  $a \sim \bar{a}$  iff there exists  $b$  in  $R$  such that  $aR + bR = R$  and  $aR \cap bR = b\bar{a}R$ , in which case  $b\bar{a} = a\bar{b}$  ( $\bar{b} \in R$ ) and  $b \sim \bar{b}$  (see Jacobson [6, p. 34] and Cohn [3]). Using the latter definition it can be verified that elements similar to units are units and elements similar to zero are zero.

Using the last remark one may prove that right Bezout domains satisfy the right Ore condition: the intersection of any two non-zero principal right ideals is non-zero. For if  $aR, bR$  are two non-zero right ideals of  $R$  then  $aR + bR = dR$  and  $aR \cap bR = mR$  for some  $d, m \in R$ ,  $d \neq 0$ . Thus  $a = d\bar{a}$ ,  $m = b\bar{m}$  for some  $\bar{a}, \bar{m} \in R$ ,  $\bar{a} \neq 0$ . It follows from  $R/aR \cong dR/d\bar{a}R = (aR + bR)/aR \cong bR/(aR \cap bR) = bR/b\bar{m}R \cong R/\bar{m}R$  that  $\bar{a} \sim \bar{m}$  and therefore  $\bar{m} \neq 0$  because  $\bar{a} \neq 0$ . This shows that  $m \neq 0$ . Integral domains which satisfy the right Ore condition are sometimes called right Ore domains. Similar remarks hold with regard to left Bezout domains and left Ore domains, i.e., every left Bezout domain is a left Ore domain.

As an example of the non-symmetry of some of the definitions we consider  $R = F[x, \sigma]$ , the ring of skew polynomials described earlier. Assume now that  $\sigma$  is not an isomorphism. Since  $R$  is a PRI domain it follows that  $R$  is a right Bezout domain and a right Ore domain. But if  $a \in F \setminus F^\sigma$ , then  $Rx \cap Rxa = 0$ . For if  $fx = gxa \neq 0$  for some  $f = b_0 + xb_1 + \dots + x^n b_n$  and  $g = c_0 + xc_1 + \dots + x^m c_m$  in  $R$ , then  $x^{n+1}b_n^\sigma = x^{m+1}c_m^\sigma a$ . Therefore  $n = m$  and  $b_n^\sigma = c_n^\sigma a$ . Hence  $a = (c_n^{-1}b_n)^\sigma$ ,

a contradiction. Therefore  $R$  is not a left Ore domain and hence neither a PLI domain nor a left Bezout domain.

We note that  $R$  is a right Bezout domain iff  $R$  is a right Ore domain and a weak Bezout domain. Also every PRI domain is a right Bezout domain. As a converse we can show that if  $R$  is a right Bezout domain in which the ascending chain condition for principal right ideals holds then  $R$  is a PRI domain. For let  $I$  be a right ideal of  $R$  and let  $a_0 \in I$ . If  $a_0 R \neq I$  let  $a_1 \in I \setminus a_0 R$ . If  $a_0 R + a_1 R \neq I$  let  $a_2 \in I \setminus (a_0 R + a_1 R)$ . Continuing this process we obtain  $a_0 R \subset a_0 R + a_1 R \subset a_0 R + a_1 R + a_2 R \subset \dots$ . Now in a right Bezout domain the sum of a finite number of principal right ideals is again a principal right ideal. Therefore the chain that we obtain is a chain of principal right ideals and hence must terminate, say,  $a_0 R + \dots + a_n R = a_0 R + \dots + a_{n+1} R = \dots$  for some integer  $n$ . This is possible only if  $a_0 R + \dots + a_n R = I$ . Consequently  $I$  is a principal right ideal.

If  $R$  is an integral domain and  $0 \neq a \in R$ , let  $[aR, bR]$  denote the set of principal right ideals  $cR$  of  $R$  such that  $aR \subset cR \subset bR$ . If  $R$  is a weak Bezout domain and  $0 \neq a \in R$  then  $[aR, R]$  is a sublattice of the lattice of all right ideals of  $R$ . Because of the Schreier Refinement Theorem (see [1, p.66]) one may speak of the longest chain in  $[aR, R]$ . If  $[aR, R]$  contains a maximal chain of finite length then the lengths of all maximal chains in  $[aR, R]$  are equal and we define  $\dim a$  (or  $\dim_R a$ ) to be this integer. If  $[aR, R]$  contains no maximal chain of finite length then  $\dim a = \infty$  (see Johnson [9]).

If  $R$  is a weak Bezout domain and  $a, \bar{a} \in R$  with  $a \sim \bar{a}$  then  $\dim a = \dim \bar{a}$ . For if  $a \sim \bar{a}$  then there exists  $b, m \in R$  such that  $aR + bR = R$ ,  $aR \cap bR = mR$  where  $m = b\bar{a}$  ( $a, \bar{a} \neq 0$ ). If  $a$  is a unit then so is  $\bar{a}$  and  $\dim a = 0 = \dim \bar{a}$ . If  $a$  is not a unit then  $b \neq 0$  and so  $m \neq 0$ . Hence  $[mR, R]$  is a modular lattice.



Then  $[aR, R] = [aR, aR + bR] \cong [aR \cap bR, bR] = [b\bar{a}R, bR] \cong [\bar{a}R, R]$  where " $\cong$ " denotes lattice isomorphism. It follows that  $\dim a = \dim \bar{a}$ .

An element  $p$  of an integral domain  $R$  is said to be a prime if  $pR$  is maximal in the set of principal right ideals of  $R$ . It is easy to prove that the definition is left-right symmetric, i.e.,  $p$  is prime iff  $Rp$  is maximal in the set of principal left ideals of  $R$ . If  $R$  is a weak Bezout domain then  $p \in R$  is prime iff  $\dim p = 1$ . It follows that in a weak Bezout domain elements similar to primes are prime.

Of interest are those elements in  $R$  that can be expressed as a (finite) product of primes. If  $0 \neq a \in R$  and  $[aR, R]$  satisfies both the ascending and the descending chain conditions then every chain in  $[aR, R]$  has finite length. Assume in addition that  $a$  is not a unit and let  $aR \subset b_nR \subset \dots \subset b_1R \subset R$  be a maximal chain in  $[aR, R]$ . Then  $b_{i+1} = b_i s_i$  for some  $s_i \in R$ ,  $i = 1, 2, \dots, n-1$  and  $a = b_n s_n$ ,  $s_n \in R$ . Thus  $a = b_1 s_1 \dots s_n$ . Evidently  $b_1$  is prime and it follows from  $R/s_1R \cong b_1 s_1 \dots s_{i-1} R / b_1 s_1 \dots s_i R$  and from the maximality of the chain that  $s_i$  is prime ( $i = 1, 2, \dots, n$ ). Therefore both chain conditions in  $[aR, R]$  guarantees that  $a$  can be written as the product of primes. As a converse we note that if  $a = p_1 \dots p_n$  is a prime factorization of  $a$ , then  $aR \subset p_1 \dots p_{n-1}R \subset \dots \subset p_1R \subset R$  is a maximal chain in  $[aR, R]$ .

The preceding remarks imply the following. If  $R$  is a weak Bezout domain and if  $0 \neq a \in R$ , then  $\dim a = n$  (where  $n$  is a positive integer) iff  $a$  is a product of  $n$  primes. In this case it is well known that the prime factorization of an element is unique up to similarity as follows (see [3]).

**Theorem 1** Let  $R$  be a weak Bezout domain. If  $a \in R$  has two prime factorizations  $a = p_1 \dots p_n = q_1 \dots q_m$  (where  $p_i, q_i$  are primes),

then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $p_i \sim q_{\pi(i)}$  ( $i = 1, 2, \dots, n$ ).

Proof. Suppose  $a = p_1 \dots p_n = q_1 \dots q_m$  where  $p_i$  and  $q_i$  are primes. We have just seen that  $n = \dim a = m$ . To prove the uniqueness up to similarity we induct on  $n$ . If  $n = 1$  there is nothing to prove. Assume  $n > 1$ . If  $p_1 R = q_1 R$  then  $q_1 = p_1 u$  for some unit  $u \in R$ . Then  $p_2 \dots p_n = u q_2 \dots q_n$  from which the theorem follows by induction. Hence we shall assume that  $p_1 R \neq q_1 R$ . Since  $R$  is a weak Bezout domain  $p_1 R \cap q_1 R = mR$  and  $p_1 R + q_1 R = dR$  for some  $m, d \in R$ . Choose  $\bar{p}_1, \bar{q}_1 \in R$  such that  $m = p_1 \bar{q}_1 = q_1 \bar{p}_1$ . Since  $p_1 R \not\subseteq dR$  and  $p_1$  is prime  $dR = R$ . Therefore  $p_1 \sim \bar{p}_1$  and  $q_1 \sim \bar{q}_1$ . Now since  $a \in p_1 R \cap q_1 R$  it follows that  $p_1 \dots p_n = p_1 \bar{q}_1 r$  and  $q_1 \dots q_n = q_1 \bar{p}_1 s$  for some  $s, r \in R$ . Then  $s = r$ ,  $p_2 \dots p_n = \bar{q}_1 r$  and  $q_2 \dots q_n = \bar{p}_1 s$ . Since  $\bar{p}_1$  and  $\bar{q}_1$  are similar to primes they must be primes. Applying induction we obtain  $p_h \sim \bar{q}_1$  and  $q_k \sim \bar{p}_1$  for some integers  $h$  and  $k$  and therefore  $p_h \sim q_1$  and  $q_k \sim p_1$ . The remaining  $p_i$ 's ( $i \neq 1, h$ ) and  $q_j$ 's ( $j \neq 1, k$ ) may be paired into similar pairs through a fixed prime factorization of  $r = s$ . QED.

**Lemma 1** Let  $R$  be a weak Bezout domain and let  $a, \bar{a} \in R$  with  $a \sim \bar{a}$ . If  $a = cd$  then there exists  $\bar{c}, \bar{d} \in R$  such that  $c \sim \bar{c}$ ,  $d \sim \bar{d}$ , and  $\bar{a} = \bar{c} \bar{d}$ .

Proof. Assume  $a \sim \bar{a}$  ( $a, \bar{a} \neq 0$ ) and  $a = cd$ ,  $c, d \in R$ . Let  $f$  be an  $R$ -module epimorphism on  $R$  onto  $R/aR$  with kernel  $\bar{a}R$ . Let  $b \in R$  such that  $f(1) = b + aR$ . Then  $R = aR + bR$  since  $f$  is an epimorphism and  $aR \cap bR = \bar{a}R$  since  $f$  has kernel  $\bar{a}R$  (see Cohn [3]). Let  $m = b\bar{a}$ . Clearly  $m \neq 0$  and hence  $[mR, R]$  is a sublattice of the lattice of all right ideals of  $R$ . It follows that  $[aR, R] \cong [mR, bR]$  (lattice

isomorphism) where the correspondence is given by  $sR \longrightarrow sR \cap bR$  if  $aR \subset sR \subset R$  and  $rR \longrightarrow rR + aR$  if  $mR \subset rR \subset bR$  (see Birkhoff [1, p.13]). Now  $aR \subset cR \subset R$  and hence there exists  $\bar{m} \in R$  such that  $\bar{m}R = cR \cap bR$ ,  $mR \subset \bar{m}R \subset bR$ , and  $\bar{m}R + aR = cR$ . Choose  $\bar{c} \in R$  such that  $\bar{m} = b\bar{c}$ . Then  $\bar{a}R \subset \bar{c}R \subset R$ . Thus  $\bar{a} = \bar{c}\bar{d}$  for some  $\bar{d} \in R$ . Now  $cR + bR = R$  and  $cR \cap bR = \bar{m}R = b\bar{c}R$ . Consequently  $c \sim \bar{c}$ . To show  $d \sim \bar{d}$  we observe that  $f(\bar{c}) = b\bar{c} + aR = \bar{m} + aR$ . Let  $\bar{f}$  be the restriction of  $f$  to  $\bar{c}R$ . Then  $\bar{f}$  is an  $R$ -module epimorphism on  $\bar{c}R$  onto  $(\bar{m}R + aR)/aR = cR/aR$  with kernel  $\bar{a}R$ . Consequently  $\bar{c}R/\bar{a}R \cong cR/aR$ . It follows that  $R/\bar{d}R \cong \bar{c}R/\bar{c}\bar{d}R = \bar{c}R/\bar{a}R \cong cR/aR = cR/cdR \cong R/dR$ . Hence  $d \sim \bar{d}$ . QED.

Using Lemma 1 we can strengthen Theorem 1 as follows.

Theorem 2 Let  $R$  be a weak Bezout domain. If  $a, \bar{a} \in R$  with  $a \sim \bar{a}$ , and if  $a = p_1 \dots p_n$ ,  $\bar{a} = q_1 \dots q_m$  where  $p_i$  and  $q_i$  are primes, then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $p_i \sim q_{\pi(i)}$  ( $i = 1, 2, \dots, n$ ).

Proof. Assume  $a, \bar{a} \in R$ ,  $a \sim \bar{a}$  and  $a = p_1 \dots p_n$  is a prime factorization of  $a$ . It follows from Lemma 1 and induction that  $\bar{a} = \bar{q}_1 \dots \bar{q}_n$  where  $p_i \sim \bar{q}_i$  ( $i = 1, 2, \dots, n$ ). In particular the  $\bar{q}_i$  are primes. Let  $\bar{a} = q_1 \dots q_m$  be any other prime factorization of  $\bar{a}$ . By Theorem 1  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $\bar{q}_i \sim q_{\pi(i)}$ . Hence  $p_i \sim q_{\pi(i)}$ . QED.

The ascending chain condition for principal right ideals holds in an integral domain  $R$  iff the ascending chain condition holds in  $[aR, R]$  for each  $0 \neq a \in R$ . If the descending chain condition holds in  $[aR, R]$  for each  $0 \neq a \in R$  then  $R$  is said to satisfy the restricted descending chain condition for principal right ideals. In this case

every descending chain of principal right ideals is either finite or descends to zero. This condition can be characterized as follows.

Lemma 2 Let  $R$  be an integral domain. The ascending chain condition for principal left ideals holds in  $R$  iff the restricted descending chain condition for principal right ideals holds in  $R$ .

Proof. Assume the ascending chain condition for principal left ideals holds in  $R$ . Let  $\dots a_i R \subset \dots \subset a_1 R \subset R$  be a descending chain such that  $\bigcap_{i=1}^{\infty} a_i R \neq \{0\}$ . Let  $b \in \bigcap_{i=1}^{\infty} a_i R$ ,  $b \neq 0$ . Then  $b = a_i r_i$  and  $a_{i+1} = a_i s_i$  for some  $r_i, s_i \in R$  ( $i = 1, 2, \dots$ ). Hence  $b = a_i r_i$  and  $b = a_{i+1} r_{i+1} = a_i s_i r_{i+1}$  implies  $s_i r_{i+1} = r_i$  since  $a_i \neq 0$ . This shows that  $R r_i \subset \dots \subset R r_{i+1} \subset \dots$ . Because of the ascending chain condition  $R r_i = R r_{i+1} = \dots$  for some integer  $k$ . It follows that  $s_i, s_{i+1}, \dots$  are units and hence  $a_i R = a_{i+1} R = \dots$ . The proof of the converse is similar. Assume the restricted descending chain condition for principal right ideals holds in  $R$ . Let  $R r_1 \subset \dots \subset R r_i \subset \dots$  be an ascending chain and let  $0 \neq b \in R r_1$ . Then  $b = a_i r_i$  and  $r_i = s_i r_{i+1}$  for some  $a_i, s_i \in R$  ( $i = 1, 2, \dots$ ). Hence  $b = a_i r_i = a_i s_i r_{i+1}$  and  $b = a_{i+1} r_{i+1}$  yields  $a_i s_i = a_{i+1}$  since  $r_{i+1} \neq 0$ . It follows that  $\dots \subset a_i R \subset \dots \subset a_1 R \subset R$  and  $0 \neq b \in \bigcap_{i=1}^{\infty} a_i R$ . By the restricted descending chain condition we obtain  $a_k R = a_{k+1} R = \dots$  and therefore  $s_i, s_{i+1}, \dots$  are units. Hence  $R r_k = R r_{k+1} = \dots$ . QED.

It is well known that the ascending chain condition for right (left) ideals is equivalent to the condition that each right (left) ideal is finitely generated. The proof of this statement is the same as in the commutative case (see Mariski and Samuel [11, p. 158] for example). It follows that if  $R$  is a PRI and a PLI domain then

$R$  satisfies the ascending chain condition for both (principal) right and left ideals. Hence  $[aR, R]$  satisfies both chain conditions for each  $0 \neq a \in R$  by Lemma 2. That is, each non-zero element in  $R$  has finite dimension. Hence each non-zero element of  $R$  that is not a unit can be factored into primes. Uniqueness of the factorization follows from Theorem 1. We state this well known result (see Jacobson [6, p. 34]) as follows.

Theorem 3 Let  $R$  be a PRI and a PLI domain. Each non-zero element of  $R$  that is not a unit can be factored into primes. This factorization is unique up to similarity (in the sense of Theorem 1).

Integral domains having the property described in Theorem 3 are called unique factorization domains (see John [3]).

## CHAPTER II

## RIGHT QUOTIENT MONOIDS

2.1 Definition and consequences

The Ore domains that were mentioned in Chapter 1 have the important property that they are contained in a right quotient field as follows. Assume  $R$  is an integral domain satisfying the right Ore condition. Let  $R^* = R \setminus \{0\}$ . The set  $K = R(R^*)^{-1} = \{ab^{-1} \mid a \in R, b \in R^*\}$  can be made into a ring under suitable operations that extend those in  $R$ . The resulting ring is a (skew) field containing  $R$ . Similar remarks apply for left Ore domains, and if  $R$  has both Ore conditions, then the two fields  $R(R^*)^{-1}$  and  $(R^*)^{-1}R$  are equal as sets and isomorphic as rings (see Jacobson [6, p. 118]).

The construction above can be generalized just as in the commutative case. We consider an integral domain  $R$ , and let  $R^* = R \setminus \{0\}$ . We shall say that a subset  $S$  of  $R^*$  has the right quotient conditions (with respect to  $R$ ) if

$$1) a, b \in S \text{ iff } ab \in S$$

$$2) a \in S, b \in R \text{ implies there exists } \bar{a} \in S, \bar{b} \in R \text{ such that } a\bar{b} = b\bar{a}.$$

Under these conditions if  $S \neq \emptyset$  then  $S$  contains the group of units of  $R$ . For if  $a \in S$  then  $1a \in S$  and so  $1 \in S$  by 1). Then for each unit  $u \in R$ ,  $1 = uu^{-1} \in S$  and so  $u \in S$  by 1). If  $S \neq \emptyset$  and has the right quotient conditions then  $S$  is called a right quotient monoid (in  $R$ ). In this case it can be shown (see Bourbaki [2, p. 162]) that the set  $K = RS^{-1} = \{rs^{-1} \mid r \in R, s \in S\}$  can be made into a ring under suitable operations that extend those in  $R$ . The resulting ring is an integral domain containing  $R$  with the property that the members of  $S$  are units

in  $K$ . Of course if  $S = R^*$ , then  $K$  is the right quotient field of  $R$  described in the last paragraph. Similar remarks apply for subsets that are left quotient monoids in  $R$ , and if  $S$  is both a left and a right quotient monoid in  $R$ , then  $S^{-1}R$  and  $RS^{-1}$  are equal as sets and isomorphic as rings.

The preceding construction is usually carried out with condition 1) replaced by the weaker condition that  $S$  be multiplicatively closed. However we shall need the full strength of condition 1), for example, in Lemma 3 to follow. We note here that condition 1) defines  $R \setminus S$  to be a prime ideal in the multiplicative monoid  $R^*$ . We also note that because of condition 1) the following special case of condition 2) is valid:  $a \in S, b \in S$  implies there exists  $\bar{a} \in S, \bar{b} \in S$  such that  $a\bar{b} = b\bar{a}$ . We shall now proceed to establish some useful properties concerning  $R$  and  $K = RS^{-1}$ .

Lemma 3 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ .

Let  $U_K, U_R$  be the group of units of  $K$  and  $R$  respectively. Then

1)  $U_K = SS^{-1}$  and 2)  $S = R \cap U_K$ .

Proof. Clearly  $SS^{-1} \subset U_K$ . Now let  $br^{-1} \in U_K$  and let  $as^{-1} \in U_K$  be its inverse ( $a, b \in R, r, s \in S$ ). Then  $as^{-1}br^{-1} = 1$ . Choose  $\bar{s} \in S, \bar{b} \in R$  such that  $b\bar{s} = s\bar{b}$ . Then  $a\bar{b}\bar{s}^{-1}r^{-1} = 1, a\bar{b} = r\bar{s}$  and so  $a, \bar{b} \in S$ . It follows from  $b\bar{s} = s\bar{b}$  that  $b\bar{s}$  and therefore  $b$  belongs to  $S$ . Therefore  $br^{-1} \in SS^{-1}$  and 1) is established. To prove 2) let  $x = br^{-1} \in R \cap U_K$ . It follows by 1) that we can choose  $b, r \in S$ . Therefore  $rx \in S$  and so  $x \in S$ . Thus  $R \cap U_K \subset S$ . The reverse inclusion is obvious. QED.

Lemma 4 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ .

If  $I$  is a right ideal of  $R$  then  $IS^{-1}$  is a right ideal of  $K$ . Conversely each right ideal  $J$  of  $K$  is of the form  $J = (J \cap R)S^{-1}$ .

Proof. Let  $I$  be a right ideal of  $R$  and let  $as^{-1}, br^{-1} \in IS^{-1}$ .

Choose  $\bar{r}, \bar{s} \in S$  such that  $s\bar{r} = r\bar{s}$ . Then

$$as^{-1} - br^{-1} = a\bar{r}(s\bar{r})^{-1} - b\bar{s}(r\bar{s})^{-1} = (a\bar{r} - b\bar{s})(r\bar{s})^{-1} \in IS^{-1}.$$

Similarly if  $as^{-1} \in IS^{-1}, br^{-1} \in K$ , then choose  $\bar{s} \in S, \bar{b} \in R$  such that  $s\bar{b} = b\bar{s}$ . Then  $b = s\bar{b}\bar{s}^{-1}$  and  $as^{-1}br^{-1} = as^{-1}(s\bar{b}\bar{s}^{-1})r^{-1} = a\bar{b}\bar{s}^{-1}r^{-1} = a\bar{b}(r\bar{s})^{-1} \in IS^{-1}$ .

Hence  $IS^{-1}$  is a right ideal of  $K$ . To show the converse let  $J$  be a right ideal of  $K$ . Clearly  $I = J \cap R$  is a right ideal of  $R$ . Now

$$IS^{-1} = (J \cap R)S^{-1} \subset JS^{-1} \subset J.$$

Also if  $z \in J$  then  $z = bs^{-1}, b \in R, s \in S$

and  $b = zs \in J$  because  $J$  is a right ideal. This shows that  $z \in IS^{-1}$ .

Therefore  $IS^{-1} = J$ , i.e.,  $(J \cap R)S^{-1} = J$ . QED.

Lemma 5 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ .

If  $A, B$  are right ideals of  $R$ , then 1)  $(A \cap B)S^{-1} = AS^{-1} \cap BS^{-1}$  and

$$2) (A + B)S^{-1} = AS^{-1} + BS^{-1}.$$

Proof. Clearly  $(A \cap B)S^{-1} \subset AS^{-1} \cap BS^{-1}$ . Now suppose

$as_1^{-1} = bs_2^{-1} \in AS^{-1} \cap BS^{-1}$  ( $s_1, s_2 \in S$ ). Choose  $\bar{s}_1, \bar{s}_2 \in S$  such that

$$s_1\bar{s}_2 = s_2\bar{s}_1. \text{ Then } a\bar{s}_2 = b\bar{s}_1 \in A \cap B. \text{ Also } as_1^{-1} = a\bar{s}_2(s_2\bar{s}_1)^{-1} \in (A \cap B)S^{-1}.$$

This proves  $AS^{-1} \cap BS^{-1} \subset (A \cap B)S^{-1}$  and 1) is established. Now it

is clear that  $(A + B)S^{-1} \subset AS^{-1} + BS^{-1}$ . To show the reverse inclusion

let  $as_1^{-1} + bs_2^{-1} \in AS^{-1} + BS^{-1}$  ( $s_1, s_2 \in S$ ) and choose  $\bar{s}_1, \bar{s}_2 \in S$  such that

$$s_1\bar{s}_2 = s_2\bar{s}_1. \text{ Then } as_1^{-1} + bs_2^{-1} = (a\bar{s}_2 + b\bar{s}_1)(s_1\bar{s}_2)^{-1} \in (A + B)S^{-1}.$$

Therefore  $AS^{-1} + BS^{-1} \subset (A + B)S^{-1}$ . QED.

Lemma 6 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ .

If  $a, \bar{a} \in R$  and  $a \sim_R \bar{a}$ , then  $a \sim_K \bar{a}$ .



Proof. Let  $a, \bar{a} \in R$  with  $a \sim_R \bar{a}$ . Then  $aR + bR = R$  and  $aR \cap bR = \bar{b}aR$  for some  $b \in R$ . Therefore  $aK + bK = K$  and  $aK \cap bK = \bar{b}aK$  by Lemma 5. Hence  $a \sim_K \bar{a}$ . QED.

Lemma 7 1) Let  $S$  be a right quotient monoid in  $R$ . If  $a \in S$ ,  $\bar{a} \in R$  with  $a \sim \bar{a}$  then  $\bar{a} \in S$ .

2) Suppose  $R$  is a right Bezout domain and  $S$  is a non-empty subset of  $R$  such that  $0 \notin S$  and  $ab \in S$  iff  $a, b \in S$ . Then  $S$  is a right quotient monoid in  $R$  iff elements similar to members of  $S$  belong to  $S$ , i.e.,  $a \in S$ ,  $\bar{a} \in R$ , and  $a \sim \bar{a}$  implies  $\bar{a} \in S$ .

Proof. To prove 1) assume  $S$  is a right quotient monoid in  $R$ ,  $K = RS^{-1}$ ,  $a \in S$ ,  $\bar{a} \in R$ , and  $a \sim_R \bar{a}$ . Then  $a \sim_K \bar{a}$  by Lemma 6. Now  $a$  is a unit in  $K$  and therefore so is  $\bar{a}$ . Consequently  $\bar{a} \in S$  by Lemma 3. To prove 2) assume  $R$  is a right Bezout domain and that  $S$  is a non-empty subset of  $R$  such that  $0 \notin S$  and  $ab \in S$  iff  $a, b \in S$ . Further assume  $a \in S$ ,  $\bar{a} \in R$ , and  $a \sim \bar{a}$  implies  $\bar{a} \in S$ . To show  $S$  is a right quotient monoid let  $a \in S$ ,  $b \in R$ . Choose  $d, m \in R$  such that  $aR + bR = dR$  and  $aR \cap bR = mR$ . Then  $a = da'$ ,  $b = db'$ , and  $m = a\bar{b} = \bar{b}a$  for some  $a', b', \bar{a}, \bar{b} \in R$ . It follows that  $a'R + b'R = R$  and  $a'R \cap b'R = b'\bar{a}R$ . Therefore  $a' \sim \bar{a}$ . Now  $a \in S$  implies  $a' \in S$  and so  $\bar{a} \in S$ . Hence  $a\bar{b} = \bar{b}a$  with  $\bar{a} \in S$ , and  $S$  is a right quotient monoid. The converse follows from 1). QED.

Lemma 8 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . If  $R$  satisfies the ascending chain condition for right ideals then so does  $K$ .

Proof. Let  $J_1 \subset \dots \subset J_i \subset \dots$  be an ascending chain of right ideals of  $K$ . Let  $I_i = J_i \cap R$ . Then  $I_1 \subset \dots \subset I_i \subset \dots$  is an ascending chain of right ideals of  $R$  which must therefore terminate. Thus

$I_k = I_{k+1} = \dots$ , for some integer  $k$ . Then  $I_k S^{-1} = I_{k+1} S^{-1} = \dots$ , and it follows from Lemma 4 that  $J_k = J_{k+1} = \dots$ . QED.

Lemma 9 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . Then  $K$  is a right Ore domain iff  $R$  is a right Ore domain.

Proof. Let  $a, b \in R^*$ . By Lemma 5  $(aR \cap bR)S^{-1} = aK \cap bK$ . Therefore  $aR \cap bR = \{0\}$  iff  $aK \cap bK = \{0\}$ . It follows that if  $K$  is a right Ore domain then so is  $R$ . The converse is obvious because  $R \subset K$ . QED.

Lemma 10 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . If  $R$  is a weak Bezout domain then so is  $K$ .

Proof. Assume  $R$  is a weak Bezout domain. Let  $a, b \in K$  such that  $aK \cap bK \neq \{0\}$ . Because  $rs^{-1}K = rK$  for any  $rs^{-1} \in K$  it suffices to consider  $a, b \in R$ . The proof of Lemma 9 shows that  $aR \cap bR \neq \{0\}$ . Therefore  $aR + bR = dR$  and  $aR \cap bR = mR$  for some  $d, m \in R$ . It follows by Lemma 5 that  $aRS^{-1} + bRS^{-1} = dRS^{-1}$  and  $aRS^{-1} \cap bRS^{-1} = mRS^{-1}$ . QED.

Since the right Bezout condition is equivalent to the weak Bezout condition together with the right Ore condition, Lemmas 9 and 10 together yield the following.

Lemma 11 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . If  $R$  is a right Bezout domain then so is  $K$ .

We have already remarked in Chapter 1 that  $R$  is a PRI domain iff  $R$  is a right Bezout domain satisfying the ascending chain condition for principal right ideals. Therefore Lemmas 9 and 11 together imply the following.

Lemma 12 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . If  $R$  is a PRI domain then so is  $K$ .

We recall that an integral domain is called a local domain if every sum of non-units is a non-unit.

Lemma 10 Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . Then  $K$  is a local domain iff  $R \setminus S$  is an ideal.

Proof. Because  $S$  has the right quotient conditions  $R \setminus S$  is an ideal in the multiplicative monoid  $R^*$ . Assume  $K$  is a local domain. To show that  $I = R \setminus S$  is an ideal in  $R$  we need only show that  $I$  is closed under subtraction. Accordingly let  $a, b \in I$ . Then  $a$  and  $-b$  are non-units in  $K$  by Lemma 3. Therefore  $a - b$  is a non-unit in  $K$ . Hence  $a - b \in I$  by Lemma 3. Thus  $I$  is an ideal of  $R$ . Conversely assume that  $I$  is an ideal of  $R$ . Let  $as^{-1}, br^{-1}$  be two non-units of  $K$  ( $s, r \in S$ ). Choose  $\bar{r}, \bar{s} \in S$  such that  $s\bar{r} = r\bar{s}$ . Then  $as^{-1} + br^{-1} = (a\bar{r} + b\bar{s})(s\bar{r})^{-1}$ . Since  $a\bar{r}, b\bar{s} \in R \setminus S = I$  and  $I$  is an ideal,  $a\bar{r} + b\bar{s} \in I$  and consequently  $(a\bar{r} + b\bar{s})(s\bar{r})^{-1}$  is a non-unit of  $K$  by Lemma 3. Hence  $as^{-1} + br^{-1}$  is a non-unit of  $K$  and  $K$  is a local domain. QED.

Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . Let  $L_R$  denote the lattice of right ideals of  $R$  and  $L_K$  the lattice of right ideals of  $K$ . We conclude this section by formalizing the relationship between  $L_R$  and  $L_K$ .

An  $S$ -closure operator  $cl$  (or  $cl_S$ ) can be defined on  $L_R$  by  $cl(I) = IS^{-1} \cap R$  for each  $I \in L_R$ . Lemma 4 shows that  $cl$  is a function on  $L_R$  into  $L_R$ . Using Lemmas 4 and 5 it is not difficult to check that  $cl$  has the following properties.

- 1)  $I \subset cl(I), I \in L_R$
- 2)  $cl(I) = cl(cl(I)), I \in L_R$
- 3)  $cl(I \cap J) = cl(I) \cap cl(J), I, J \in L_R$
- 4)  $cl(I) + cl(J) \subset cl(I + J), I, J \in L_R$

We say that  $I \in L_R$  is closed (or S-closed) if  $I = \text{cl}(I)$ . It follows that  $\text{cl}(I)$  is the smallest closed right ideal of  $R$  that contains  $I$ . Let  $L_R'$  denote the set of closed right ideals of  $R$ . Clearly  $0, R \in L_R'$  and  $L_R'$  is a lattice under inclusion. If  $I, J \in L_R'$  then  $I \wedge J$  is the inf of  $I$  and  $J$ . We denote the sup of  $I$  and  $J$  by  $I \vee J$ ; thus  $I \vee J = \text{cl}(I + J)$ .

Theorem 4. Let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . Let  $L_K$  be the lattice of right ideals of  $K$  and  $L_R'$  the lattice of  $S$ -closed right ideals of  $R$ . Then  $L_K \cong L_R'$ .

Proof. We recall from [1, p. 24] that two lattices  $L_1$  and  $L_2$  are isomorphic iff there is a function  $f: L_1 \rightarrow L_2$  defined on  $L_1$  onto  $L_2$  such that both  $f$  and  $f^{-1}$  are order preserving bijections. Accordingly we define the function  $f: L_K \rightarrow L_R'$  by  $I^f = I \wedge R$  for each  $I \in L_K$ . If  $I \in L_K$  then  $(I \wedge R) \in L_R'$  because  $\text{cl}(I \wedge R) = (I \wedge R)S^{-1} \wedge R = I \wedge R$  by Lemma 4. Now  $f$  is injective, for if  $I, J \in L_K$  and  $I^f = J^f$  then  $I \wedge R = J \wedge R$ ,  $(I \wedge R)S^{-1} = (J \wedge R)S^{-1}$  and so  $I = J$  by Lemma 4. Also  $f$  is surjective because if  $I \in L_R'$  then  $I = \text{cl}(I) = IS^{-1} \wedge R$  which shows that  $I = (IS^{-1})^f$ . It follows that  $f^{-1}$  is a bijection defined on  $L_R'$  and is given by  $I^{f^{-1}} = IS^{-1}$  for each  $I \in L_R'$ . Now  $I \subset J$  iff  $I^f \subset J^f$  because if  $I, J \in L_K$  then  $I \subset J$  implies  $I \wedge R \subset J \wedge R$  which implies  $(I \wedge R)S^{-1} \subset (J \wedge R)S^{-1}$  which implies  $I \subset J$ . It follows that  $f$  and  $f^{-1}$  are order preserving. Consequently  $L_K \cong L_R'$ . QED.

## 2.2 Unique factorization

In this section we shall prove the Factorization theorem. This theorem is one of our key results and has important application in the next chapter. We begin with the following result which will be used to prove the Factorization theorem.

Factorization lemma    Let  $S$  be a right quotient monoid in an integral domain  $R$ .

1) If  $R$  satisfies the ascending chain condition for principal right ideals, then each  $z \in R^*$  can be written as  $z = xs$  where  $s \in S$  and  $x$  has no non-unit right factor in  $S$ .

2) If  $R$  is a weak Bezout domain and if  $z = x_1 s_1 = x_2 s_2$  are two factorizations of  $z$  as in 1) then there is a unit  $u \in R$  such that  $x_1 = x_2 u$  (and  $us_1 = s_2$ ).

Proof. To prove 1) assume that  $R$  satisfies the ascending chain condition for principal right ideals. Let  $z \in R^*$ . If  $z$  has no non-unit right factor in  $S$  then we are finished. Otherwise  $z = x_1 s_1$  where  $s_1$  is a non-unit in  $S$ . If  $x_1$  has no non-unit right factor in  $S$  then we are finished. Otherwise  $x_1 = x_2 s_2$  where  $s_2$  is a non-unit in  $S$ . Continuing this process we obtain the chain  $x_1 R \subset x_2 R \subset \dots$  which must terminate. Thus  $x_k R = x_{k+1} R = \dots$  for some integer  $k$ . Now this is possible iff  $x_k$  has no non-unit right factor in  $S$ . Therefore  $z = x_k (s_k \dots s_1)$  is the desired factorization.

To prove 2) assume that  $R$  is a weak Bezout domain. Let  $0 \neq z \in R$  and let  $z = x_1 s_1 = x_2 s_2$  be two factorizations of  $z$  such that  $s_1, s_2 \in S$  and  $x_1, x_2$  have no non-unit right factors in  $S$ . Since  $x_1 R \cap x_2 R \neq 0$  and since  $R$  is a weak Bezout domain it follows that  $x_1 R \cap x_2 R = mR$  and

$x_1 R + x_2 R = dR$  for some  $m, d \in R$ . Then  $m = x_1 \bar{x}_2 = x_2 \bar{x}_1$  for some  $\bar{x}_1, \bar{x}_2 \in R$ . Since  $z \in x_1 R \wedge x_2 R$  there exists  $z_1, z_2 \in R$  such that  $x_1 z_1 = x_1 \bar{x}_2 z_1$  and  $x_2 z_2 = x_2 \bar{x}_1 z_2$ . Hence  $s_1 = \bar{x}_2 z_1$  and  $s_2 = \bar{x}_1 z_2$ . This shows that  $\bar{x}_1, \bar{x}_2 \in S$ . Now  $x_1 R + x_2 R = dR$  implies that  $x_1 = dx_1'$  and  $x_2 = dx_2'$  for some  $x_1', x_2' \in R$ . It follows that  $x_1' R + x_2' R = R$ ,  $x_1' R \wedge x_2' R = x_1' \bar{x}_2 R$  and  $x_1' \bar{x}_2 = x_2' \bar{x}_1$ . Therefore  $x_1' \sim \bar{x}_1$  and  $x_2' \sim \bar{x}_2$ . Since  $\bar{x}_1, \bar{x}_2 \in S$ ,  $x_1', x_2' \in S$  by Lemma 7. Now  $x_1$  and  $x_2$  have no non-unit right factors in  $S$  and consequently  $x_1'$  and  $x_2'$  must be units. This shows that  $x_1 R = dR = x_2 R$  and 2) is established. QED.

Let  $R$  be a PRI domain, let  $S$  be a right quotient monoid in  $R$  and let  $K = RS^{-1}$ . Using the Factorization lemma it is possible to characterize the elements  $a \in R$  such that  $aR$  is  $S$ -closed. If  $a \in R^*$  then  $a = \bar{a}s$  where  $s \in S$  and  $\bar{a}$  has no non-unit right factor that belongs to  $S$ . Then  $cl(aR) = aR \wedge R = \bar{a}R \wedge R = cl(\bar{a}R)$ . Now  $\bar{a}R$  is closed for if  $a'R = \bar{a}R \wedge R$  then  $\bar{a}R \subset a'R$ . Hence  $\bar{a} = a'r$  for some  $r \in R$ . But since  $\bar{a}R = a'R$   $r$  must be a unit in  $K$ , i.e.,  $r \in S$ . However  $\bar{a}$  has no non-unit right factor in  $S$  and so  $r$  is a unit in  $R$ . Therefore  $\bar{a}R = a'R = cl(\bar{a}R)$ . We conclude that if  $a \in R^*$  then  $aR$  is  $S$ -closed iff  $a$  has no non-unit right factor in  $S$ .

Let  $R$  be an integral domain. Let  $I = \{\alpha \mid 0 \leq \alpha \leq \alpha_0\}$  be an initial segment of ordinals. A collection  $\{S_\alpha \mid \alpha \in I\}$  of right quotient monoids in  $R$  is called a right quotient chain (in  $R$ ) if the following conditions hold.

- 1)  $S_\alpha \subsetneq S_{\alpha+1}$  for each  $\alpha \in I$ ,  $\alpha \neq \alpha_0$
- 2)  $S_\alpha = \bigcup_{\beta < \alpha} S_\beta$  if  $\alpha$  is a limit ordinal.

For convenience we let  $S_{-1}$  denote the group of units of  $R$ . Then  $S_{-1}$  is

contained in each  $S_\alpha$ . Let  $K_\alpha = R(S_\alpha)^{-1}$  if  $\alpha = -1$  or if  $\alpha \in I$ . Then because of condition 1)  $K_{\alpha-1} \subset K_\alpha$  for each  $\alpha \in I$ .

Factorization theorem Let  $R$  be a weak Bezout domain satisfying the ascending chain condition for principal right ideals. Let  $I = \{\alpha \mid 0 \leq \alpha \leq \alpha_0\}$  be an initial segment of ordinals and let  $\{S_\alpha \mid \alpha \in I\}$  be a right quotient chain in  $R$ . Each  $z \in R^*$  can be factored as  $z = ra_{\alpha_1} \dots a_{\alpha_n}$  where  $\alpha_i$  are non-limit ordinals such that  $\alpha_0 \geq \alpha_1 > \dots > \alpha_n$ ,  $a_{\alpha_i} \in S_{\alpha_i}$ ,  $a_{\alpha_i}$  has no non-unit right factor in  $S_{\alpha_i-1}$ ,  $r \in R^*$  and  $r$  has no non-unit right factor in  $S_{\alpha_0}$ . The factorization is unique in the sense that if  $z = sb_{\beta_1} \dots b_{\beta_m}$  is another such factorization then  $n = m$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, n$ ), and there are units  $u_0, u_1, \dots, u_{n-1}$  in  $R$  such that  $r = su_0$ ,  $a_{\alpha_n} = u_{n-1}^{-1} b_{\alpha_n}$ , and  $a_{\alpha_i} = u_{i-1}^{-1} b_{\alpha_i} u_i$  ( $i \neq 0, n$ ).

Proof. To prove existence of the factorization let  $z \in R^*$ . If  $z$  has no non-unit right factor in  $S_{\alpha_0}$  then we are finished. Otherwise by the Factorization lemma  $z = rs_0$  for some  $s_0 \in S_{\alpha_0}$  and where  $r$  has no non-unit right factor in  $S_{\alpha_0}$ . Let  $\alpha_1$  be the least ordinal such that  $s_0 \in S_{\alpha_1}$ . Clearly  $\alpha_1$  is not a limit ordinal and  $\alpha_0 \geq \alpha_1$ . By the Factorization lemma it follows that  $s_0 = a_{\alpha_1} s_1$  where  $s_1 \in S_{\alpha_1-1}$  and  $a_{\alpha_1}$  has no non-unit right factor in  $S_{\alpha_1-1}$ . Clearly  $a_{\alpha_1} \in S_{\alpha_1}$  because  $s_0 \in S_{\alpha_1}$ . If  $s_1$  is not a unit let  $\alpha_2$  be the least ordinal such that  $s_1 \in S_{\alpha_2}$ . Then  $\alpha_1 > \alpha_2$  and  $\alpha_2$  is not a limit ordinal. Another application of the Factorization lemma yields  $s_1 = a_{\alpha_2} s_2$  where  $s_2 \in S_{\alpha_2-1}$  and  $a_{\alpha_2}$  has no non-unit right factor in  $S_{\alpha_2-1}$ . Clearly  $a_{\alpha_2} \in S_{\alpha_2}$ . If  $s_2$  is not a unit we may repeat the process. Now the process cannot continue indefinitely since we would obtain an infinite sequence  $\alpha_1 > \alpha_2 > \dots$

contradicting the well ordering of the ordinals. Thus the process stops, say, with the integer  $n$ . That is,  $a_{\alpha_n}$  has no non-unit right factor in  $S_{\alpha_n-1}$  and  $s_n$  is a unit. This establishes existence of the factorization.

To prove uniqueness suppose  $z = ra_{\alpha_1} \dots a_{\alpha_n} = sb_{\beta_1} \dots b_{\beta_m}$  are two factorizations of  $z$  of the type stated in the theorem. Then the second part of the Factorization lemma applies and yields  $r = su_0$  for some unit  $u_0 \in R$ . Therefore  $a_{\alpha_1} \dots a_{\alpha_n} = u_0^{-1}b_{\beta_1} \dots b_{\beta_m}$ . Evidently  $\alpha_1 = \beta_1$ . Again the second part of the Factorization lemma applies and yields  $\alpha_1 = u_0^{-1}b_{\beta_1}u_1$  for some unit  $u_1 \in R$ . Cancelling this factor we obtain  $a_{\alpha_2} \dots a_{\alpha_n} = u_1^{-1}b_{\beta_2} \dots b_{\beta_m}$ . Uniqueness now follows by induction. QED.



## CHAPTER III

## APPLICATION TO ARBITRARY ELEMENTS IN A PRI DOMAIN

3.1 Unique factorization and infinite primes

In this section we shall construct a natural set  $\{R^{(\alpha)} \mid \alpha \in I\}$  which is a right quotient chain in a right Bezout domain  $R$ . We shall then apply the Factorization theorem to this right quotient chain. We begin by characterizing the peculiar factors that appear in the Factorization theorem. For this purpose we make the following definition.

Definition Let  $I = \{\alpha \mid 0 \leq \alpha \leq \alpha_0\}$  be an initial segment of ordinals and let  $\{S_\alpha \mid \alpha \in I\}$  be a right quotient chain in an integral domain  $R$ . For each non-limit ordinal  $\alpha \in I$  an element  $x \in S_\alpha$  is called an  $\alpha$ -prime if  $xR$  is maximal in  $\{xR \mid x \in S_\alpha \setminus S_{\alpha-1}\}$ .

Lemma 14 Let  $I = \{\alpha \mid 0 \leq \alpha \leq \alpha_0\}$  be an initial segment of ordinals and let  $\{S_\alpha \mid \alpha \in I\}$  be a right quotient chain in a PRI domain  $R$ . If  $\alpha$  is a non-limit ordinal in  $I$  and  $x$  is an  $\alpha$ -prime then  $x$  is prime in  $K_{\alpha-1}$ .

Proof. Assume the hypotheses and let  $x$  be an  $\alpha$ -prime. Suppose  $xK_{\alpha-1} \subsetneq yK_{\alpha-1} \subsetneq K_{\alpha-1}$ . Then  $xR \subsetneq xK_{\alpha-1} \cap R \subsetneq yK_{\alpha-1} \cap R \subsetneq R$ . Let  $\bar{y} \in R$  be such that  $\bar{y}R = yK_{\alpha-1} \cap R$ . Then  $xR \subsetneq \bar{y}R$ . The definition of  $\alpha$ -prime implies that  $\bar{y} \in S_{\alpha-1}$  and therefore  $\bar{y}$  is a unit in  $K_{\alpha-1}$  and  $\bar{y}K_{\alpha-1} = K_{\alpha-1}$ . Now  $\bar{y}K_{\alpha-1} = yK_{\alpha-1}$  and so  $yK_{\alpha-1} = K_{\alpha-1}$ . This shows that  $x$  is prime in  $K_{\alpha-1}$ . QED.

Lemma 15 Let  $R$  be a weak Bezout domain, let  $I$  be an initial segment of ordinals, and let  $\{S_\alpha \mid \alpha \in I\}$  be a right quotient chain in  $R$ . If  $x_1, \dots, x_k$  are  $\angle$ -primes, then  $x_1 \dots x_k$  has no non-unit right factor that belongs to  $S_{\angle-1}$ .

Proof. The proof is by induction on  $k$ . The lemma is true if  $k = 1$  by the definition of  $\angle$ -prime. Assume  $k$  is an integer greater than 1 and the lemma holds for positive integers less than  $k$ . Suppose  $x_1 \dots x_k = ab$  with  $b \in S_{\angle-1}$ ,  $a \in R$  and  $x_i$  are  $\angle$ -primes. We shall show that  $b$  must be a unit. If  $aR \subset x_1 R$  then  $a = x_1 s$ ,  $s \in R$ . Hence  $x_2 \dots x_k = sb$ . By induction it follows that  $b$  must be a unit. Suppose on the other hand that  $aR \not\subset x_1 R$ . Then since  $x_1 R \cap aR \neq \{0\}$  and  $R$  is a weak Bezout domain it follows that  $x_1 R + aR = dR$  and  $x_1 R \cap aR = mR$  for some  $d, m \in R$ . Choose  $x', a', \bar{a}, \bar{x}_1 \in R$  such that  $x_1 = dx'$ ,  $a = da'$ , and  $m = x_1 \bar{a} = a \bar{x}_1$ . Then  $x'R + a'R = R$ ,  $x'R \cap a'R = a' \bar{x}_1 R$ . Consequently  $x' \sim \bar{x}_1$ . Now  $x_1 \dots x_k = x_1 \bar{a} z$  for some  $z \in R$ . Therefore  $ab = x_1 \dots x_k = x_1 \bar{a} z$  and so  $b = \bar{x}_1 z$ . Hence  $z \in S_{\angle-1}$  since  $b \in S_{\angle-1}$ . It follows from  $x_2 \dots x_k = \bar{a} z$  and by induction that  $z$  is a unit. Consequently  $b$  is a right associate of  $\bar{x}_1$ . Therefore  $x' \sim \bar{x}_1$  yields  $x' \sim b$  and hence  $x' \in S_{\angle-1}$  by Lemma 7. Now  $d \in S_{\angle-1}$  because  $x_1 R \subset dR$ . Therefore  $x_1 = dx' \in S_{\angle-1}$ . However this contradicts the fact that  $x_1$  is an  $\angle$ -prime. QED.

Whenever  $R$  is a weak Bezout domain  $R'$  will denote the set of finite dimensional elements of  $R$ . With additional hypotheses we are able to state a converse to Lemma 15 as follows.

Lemma 16 Let  $R$  be a weak Bezout domain satisfying the ascending chain condition for principal right ideals. Let  $I$  be an initial segment of ordinals and let  $\{S_\alpha \mid \alpha \in I\}$  be a right quotient

chain in  $R$ . Let  $\alpha$  be a non-limit ordinal in  $I$  and assume that  $S_\alpha \subset (K_{\alpha-1})'$ . If  $a \in S_\alpha$  has no non-unit right factor that belongs to  $S_{\alpha-1}$  then  $a$  is a product of  $\alpha$ -primes.

**Proof.** Assume the hypotheses. Since  $a \in S_\alpha \setminus S_{\alpha-1}$  we may choose  $x_1$  (by the ascending chain condition for principal right ideals) such that  $x_1 R$  is maximal in  $\{xR \mid xR \subset aR \text{ and } x \in S_\alpha \setminus S_{\alpha-1}\}$ . Then  $x_1$  is an  $\alpha$ -prime and  $a = x_1 s_1$  for some  $s_1 \in R$ . Obviously  $s_1 \in S_\alpha$  and if  $s_1$  is not a unit then  $s_1 \in S_\alpha \setminus S_{\alpha-1}$  because of the assumption on  $a$ . We repeat the argument and obtain  $s_1 = x_2 s_2$  where  $x_2$  is an  $\alpha$ -prime and  $s_2 \in S_\alpha$ . If this process does not terminate we obtain, for each positive integer  $i$ ,  $s_i = x_{i+1} s_{i+1}$  where  $x_{i+1}$  is an  $\alpha$ -prime. Since each  $x_i$  is a non-unit in  $K_{\alpha-1}$  by Lemma 3 we obtain  $K_{\alpha-1} a \subsetneq K_{\alpha-1} s_1 \subsetneq K_{\alpha-1} s_2 \subsetneq \dots$ . The proof of Lemma 2 then shows that  $\dim_{K_{\alpha-1}} a = \infty$ , contradicting  $a \in (K_{\alpha-1})'$ . Therefore the process terminates, say, with the integer  $k$ . Thus  $a = x_1 \dots x_k s_k$  and  $s_k$  is a unit in  $R$ . QED.

Each right Bezout domain contains a natural right quotient monoid as follows.

**Lemma 17** Let  $R$  be a right Bezout domain. Then  $R' = \{a \in R \mid \dim a < \infty\}$  is a right quotient monoid.

**Proof.** Clearly  $0 \notin R'$  and  $1 \in R'$ . Also  $a \in R'$ ,  $\bar{a} \in R$  and  $a \sim \bar{a}$  implies  $\dim a = \dim \bar{a}$  and hence  $\bar{a} \in R'$ . Suppose  $a, b \in R$  and we may assume that  $a, b \neq 0$ . Then  $aR/abR \cong R/bR$  and therefore  $\dim ab = \dim a + \dim b$ . Hence  $ab \in R'$  iff  $a, b \in R'$ . It follows by the second part of Lemma 7 that  $R'$  is a right quotient monoid in  $R$ . QED.

Let  $R$  be a right Bezout domain. We construct, by transfinite induction, a natural chain  $\{R^{(\alpha)} \mid \alpha \text{ is an ordinal}\}$  of right quotient monoids in  $R$  as follows.

Let  $R^{(0)} = R'$ . Let  $\alpha$  be an ordinal greater than zero and assume  $R^{(\beta)}$  has been defined and is a right quotient monoid whenever  $\beta < \alpha$ , and let  $K_\beta = R(R^{(\beta)})^{-1}$ . By Lemma 11  $K_\beta$  is a right Bezout domain and therefore  $K_\beta'$  is a right quotient monoid in  $K$  by Lemma 17 ( $\beta < \alpha$ ). We define  $R^{(\alpha)}$  by

$$R^{(\alpha)} = \bigcup_{\beta < \alpha} R^{(\beta)} \text{ if } \alpha \text{ is a limit ordinal}$$

$$R^{(\alpha)} = (K_{\alpha-1})' \cap R \text{ if } \alpha \text{ is not a limit ordinal.}$$

To show that the induction is valid we must show that  $R^{(\alpha)}$  is a right quotient monoid. If  $\alpha$  is a limit ordinal the proof is obvious. Assume that  $\alpha$  is not a limit ordinal. Obviously  $0 \notin R^{(\alpha)}$  and  $1 \in R^{(\alpha)}$ . Also  $ab \in R^{(\alpha)}$  iff  $a, b \in R^{(\alpha)}$  because  $(K_{\alpha-1})'$  has this property. Now if  $a \in R^{(\alpha)}$ ,  $\bar{a} \in R$ , and  $a \sim_R \bar{a}$  then  $a \sim_{K_{\alpha-1}} \bar{a}$  by Lemma 6. Since  $a \in (K_{\alpha-1})'$  it follows that  $\dim_{K_{\alpha-1}} a = \dim_{K_{\alpha-1}} \bar{a}$  and  $\bar{a} \in (K_{\alpha-1})'$ . Hence  $\bar{a} \in R^{(\alpha)}$ . The hypotheses for the second part of Lemma 7 are satisfied and therefore  $R^{(\alpha)}$  is a right quotient monoid. QED.

If  $\alpha, \beta$  are ordinals such that  $\alpha \leq \beta$ , then  $R^{(\alpha)} \subset R^{(\beta)} \subset R$ . Also  $R^{(\alpha)} = R^{(\alpha+1)}$  for some ordinal  $\alpha$ . For if  $R^{(\alpha)} \neq R^{(\alpha+1)}$  for each ordinal  $\alpha$  then  $\text{card}(R^{(\alpha)}) \geq \text{card}(\alpha)$  for each ordinal  $\alpha$ . Choosing  $\beta$  such that  $\text{card}(\beta) > \text{card}(R)$  we obtain  $\text{card}(\beta) > \text{card}(R) \geq \text{card}(R^{(\beta)})$ , a contradiction. We let  $\alpha_0$  denote the least ordinal such that  $R^{(\alpha_0)} = R^{(\alpha_0+1)}$ , and we call  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  the right D-chain (Dimension chain) in  $R$ .

Evidently the right D-chain in a right Bezout domain  $R$  is a right quotient chain in  $R$ . If  $R$  is a PRI domain then the right D-chain has an additional property as follows.

Lemma 18 Let  $R$  be a PRI domain and let  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  be the right D-chain in  $R$ . Then  $R^{(\alpha_0)} = R^*$ .

Proof. Suppose  $R^* \neq R^{(\alpha_0)}$ . Then by the maximum condition in the PRI domain  $R$  we may choose  $x$  such that  $xR$  is maximal in  $\{xR \mid x \in R^* \setminus R^{(\alpha_0)}\}$ . The proof of Lemma 14 can be used to show that  $x$  is prime in  $K_{\alpha_0} = R(R^{(\alpha_0)})^{-1}$ . In particular  $x \in (K_{\alpha_0})'$  and so  $x \in (K_{\alpha_0})' \cap R = R^{(\alpha_0+1)}$ . This contradicts  $R^{(\alpha_0+1)} = R^{(\alpha_0)}$ . Therefore  $R^* = R^{(\alpha_0)}$ . QED.

Definition Let  $R$  be a PRI domain and let  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  be the right D-chain in  $R$ . We shall call the  $\alpha$ -primes in  $R$   $\inf^{(\alpha)}$  primes (where  $\alpha$  is an ordinal such that  $\alpha \leq \alpha_0$ ). For each such ordinal  $\alpha$  other than zero let  $Z^{(\alpha)}$  be the set of (finite) products of  $\inf^{(\alpha)}$  primes. Let  $Z^{(0)} = R^{(0)}$ .

Let  $R$  be a PRI domain and let  $\alpha$  be a non-limit ordinal with  $\alpha \leq \alpha_0$ . If  $xR$  is maximal in  $\{xR \mid x \in R \setminus R^{(\alpha-1)}\}$  then the proof of Lemma 14 can be used to show that  $x$  is prime in  $K_{\alpha-1}$ . In particular  $x \in (K_{\alpha-1})' \cap R = R^{(\alpha)}$  and therefore  $x$  is an  $\inf^{(\alpha)}$  prime. Hence  $x \in R$  is an  $\inf^{(\alpha)}$  prime iff  $xR$  is maximal in  $\{xR \mid x \in R \setminus R^{(\alpha-1)}\}$ . As a consequence we note that  $\inf^{(\alpha)}$  primes exist for each  $\alpha \leq \alpha_0$  by the maximum condition in  $R$ . In fact for each  $z \notin R^{(\alpha-1)}$ ,  $zR \subset xR$  for some  $\inf^{(\alpha)}$  prime  $x$ .

If  $R$  is a PRI domain we can combine Lemmas 15 and 16 into the following.

Lemma 19 Let  $R$  be a PRI domain and let  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  be the right D-chain in  $R$ . Let  $\alpha$  be a non-limit ordinal such that  $\alpha \leq \alpha_0$ , and let  $z \in R^{(\alpha)}$ . Then  $z$  has no non-unit right factor in  $R^{(\alpha-1)}$  iff  $z \in Z^{(\alpha)}$ , i.e., iff  $z$  is a product of  $\inf^{(\alpha)}$  primes.

Using Lemmas 18 and 19 we can state the Factorization theorem for the present case as follows.

Theorem 5 Let  $R$  be a PRI domain and let  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  be the right D-chain in  $R$ . Each  $a \in R^*$  can be written as  $a = z_{\alpha_1} \cdots z_{\alpha_k}$  where  $\alpha_i$  are non-limit ordinals such that  $\alpha_0 \geq \alpha_1 > \cdots > \alpha_k$  and  $z_{\alpha_i} \in Z^{(\alpha_i)}$ . This factorization is unique in the sense that if  $a = y_{\beta_1} \cdots y_{\beta_h}$  is another such factorization of  $a$  then  $h = k$ ,  $\alpha_i = \beta_i$  ( $i = 1, 2, \dots, k$ ), and there are units  $u_1, \dots, u_{k-1}$  in  $R$  such that  $z_{\alpha_1} = y_{\alpha_1} u_1$ ,  $z_{\alpha_k} = u_{k-1}^{-1} y_{\alpha_k}$ , and  $z_{\alpha_i} = u_{i-1}^{-1} y_{\alpha_i} u_i$  ( $i \neq 1, k$ ).

### 3.2 the local case

In this section we assume that  $R$  is a PRI domain, and

$\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$  denotes the right D-chain in  $R$ . We continue to use the notation  $K_\alpha = R(R^{(\alpha)})^{-1}$  whenever  $\alpha \leq \alpha_0$ . If  $\alpha, \beta$  are ordinals with  $\beta < \alpha$ , we let  $[\beta, \alpha], (\beta, \alpha), [\beta, \alpha), (\beta, \alpha]$  denote the usual intervals in the collection of ordinals. If  $J$  is one of these intervals  $J^*$  will denote the set of elements in  $J$  that are not limit ordinals. The term "unique" will mean "unique up to right unit factor."

Theorem 6 Let  $R$  be a PRI domain. Suppose  $R$  has a unique  $\inf^{(1)}$  prime  $x$ , and suppose  $xR \subset pR$  for each prime  $p$  in  $R$ . Then  $R$  is not a left Ore domain.

Proof. If  $R$  is a left Ore domain then since  $R$  is a weak Bezout domain it must be a left Bezout domain. Let  $p$  be a prime in  $R$ . Choose  $d, m, p', x' \in R$  such that  $Rx + Rp = Rd$ ,  $Rx \cap Rp = Rm$ , and  $m = p'x = x'p$ . Now  $d$  is a unit, for either  $Rd = Rp$  or  $Rd = R$  because  $p$  is prime. However if  $Rd = Rp$  then  $x$  would have  $p$  as a right factor contradicting  $x$  being an  $\inf^{(1)}$  prime (see Lemma 19). It follows that  $Rd = R$ . Therefore  $x \sim x'$  and  $p \sim p'$ . Hence  $p'$  is prime, and  $\dim x' = \dim x = \infty$ . Since  $x'R \subset yR$  for some  $\inf^{(1)}$  prime  $y$  by the maximum condition in  $R$ , it follows that  $x'R \subset xR$ . Thus  $x' = xs$  for some  $s \in R$ . Now  $p'R + x'R = R$ , otherwise  $p'R + x'R = p'R$  because  $p'$  is prime. This would imply  $x' = p'z$  for some  $z \in R$  and together with  $p'x = x'p$  would yield  $x = zp$ , contradicting  $x$  being an  $\inf^{(1)}$  prime (see Lemma 19). It follows that  $R = p'R + x'R \subset p'R + xR$  and therefore  $p'R + xR = R$ . Hence  $xR \not\subset p'R$ , and this contradicts the hypotheses. QED.

Lemma 20 Let  $R$  be a PRI domain. Suppose  $\beta \in [0, \alpha_0]^*$  and  $R$  has a unique  $\inf^{(\beta)}$  prime. Then  $R$  has a unique  $\inf^{(\alpha)}$  prime for each  $\alpha \in [\beta, \alpha_0]^*$ .

Proof. Because of the maximum condition in  $R$ ,  $\inf^{(\alpha)}$  primes exist for each  $\alpha \in [0, \alpha_0]^*$ . To prove that the  $\inf^{(\alpha)}$  primes are unique if  $\alpha \in [\beta, \alpha_0]^*$  we use transfinite induction. Let  $\alpha \in (\beta, \alpha_0]^*$  and assume  $R$  has a unique  $\inf^{(\delta)}$  prime whenever  $\delta \in [\beta, \alpha)^*$ . Let  $y, z$  be two  $\inf^{(\alpha)}$  primes in  $R$  and suppose  $yR \neq zR$ . Let  $d \in R$  such that  $dR = yR + zR$ . We claim that if  $\delta \in [\beta, \alpha)^*$  then  $d \in R \setminus R^{(\delta)}$ . For suppose  $\delta \in [\beta, \alpha)^*$  and let  $x$  be the unique  $\inf^{(\delta)}$  prime in  $R$ . Now  $yR \subset aR$  for some  $\inf^{(\delta)}$  prime  $a$  in  $R$  (by the maximum condition) and hence  $yR \subset xR$ . In fact,  $yR \subset \bigcap_{n=0}^{\infty} x^n R$  for otherwise we can choose the largest integer  $n$  such that  $yR \subset x^n R$ . Then  $y = x^n s$  for some  $s \in R \setminus xR$ . It follows that  $s \in R^{(\delta-1)}$  (otherwise  $sR \subset xR$  by the maximum condition). Hence  $y = x^n s \in R^{(\delta)}$  which contradicts the fact that  $y$  is an  $\inf^{(\alpha)}$  prime. Therefore  $yR \subset \bigcap_{n=0}^{\infty} x^n R$ . Similarly  $zR \subset \bigcap_{n=0}^{\infty} x^n R$ , and hence  $dR \subset \bigcap_{n=0}^{\infty} x^n R$ . Then  $dK_{\delta-1} \subset \bigcap_{n=0}^{\infty} x^n K_{\delta-1}$  and hence  $\dim_{K_{\delta-1}} d = \infty$ . This shows that  $d \notin (R_{\delta-1})'$  and so  $d \in R \setminus R^{(\delta)}$ . This establishes our claim that  $\delta \in [\beta, \alpha)^*$  implies  $d \in R \setminus R^{(\delta)}$ . Now  $d \in R^{(\alpha-1)}$  because  $yR \subsetneq dR$  and  $y$  is an  $\inf^{(\alpha)}$  prime. If  $\alpha-1$  is not a limit ordinal we have contradicted the claim. If  $\alpha-1$  is a limit ordinal then  $\beta < \alpha-1$  because  $\beta < \alpha$  and  $\beta$  is not a limit ordinal. Hence  $R^{(\alpha-1)} = \bigcup_{\beta \leq \delta < \alpha-1} R^{(\delta)}$  and we may choose  $\delta \in [\beta, \alpha-1)^*$  such that  $d \in R^{(\delta)}$ . Again this contradicts the claim. It follows that  $yR = zR$ . QED.

Lemma 21 Let  $R$  be a PRI domain and let  $\alpha \in [0, \alpha_0)$  or  $\alpha = -1$ . Then  $K_\alpha$  is a local domain iff  $R$  has a unique  $\inf^{(\alpha+1)}$  prime.

Proof. Suppose  $K_\alpha$  is a local domain. Then by Lemma 13  $R \setminus R^{(\alpha)}$  is an ideal, say,  $R \setminus R^{(\alpha)} = xR$ . Let  $z$  be an  $\inf^{(\alpha+1)}$  prime in  $R$ . Then



$z \in R \setminus R^{(\alpha)} = xR$  and  $zR \subset xR$ . Hence  $zR = xR$  since  $z$  is an  $\inf^{(\alpha+1)}$  prime. To prove the converse assume that  $R$  has a unique  $\inf^{(\alpha+1)}$  prime  $x$ . Then  $x$  is prime in  $K$  by Lemma 14. Let  $z$  be any prime in  $K$ . Let  $\bar{z} \in R$  such that  $\bar{z}R = zK_\alpha \wedge R$ . Then clearly  $\bar{z}K_\alpha = zK_\alpha$ . Now  $\bar{z}R \subset xR$  by the maximum condition in  $R$  and so  $\bar{z}K_\alpha \subset xK_\alpha$  and  $zK_\alpha \subset xK_\alpha$ . Hence  $zK_\alpha = xK_\alpha$  since  $z$  is prime in  $K_\alpha$ . It follows that  $K_\alpha$  is a PRI domain with a unique prime. Consequently  $K_\alpha$  is a local domain. QED.

Theorem 7 Let  $R$  be a PRI domain. Suppose  $\beta \in [0, \alpha_0)$  or  $\beta = -1$  and  $K_\beta$  is a local domain. Then  $K_\alpha$  is a local domain for each  $\alpha \in [\beta+1, \alpha_0]$ , and if  $\beta+1 < \alpha_0$ , then  $R$  is not a left Ore domain.

Proof. Since  $K_\beta$  is a local domain  $R$  has a unique  $\inf^{(\beta+1)}$  prime by Lemma 21. It follows by Lemma 20 that  $R$  has a unique  $\inf^{(\alpha)}$  prime for each  $\alpha \in [\beta+1, \alpha_0]^*$ . Therefore  $K_\alpha$  is local for each  $\alpha \in [\beta+1, \alpha_0]^*$  by Lemma 21. If  $\alpha \in [\beta+1, \alpha_0]$  and is a limit ordinal then  $K_\alpha = \bigcup_{\beta+1 \leq \gamma < \alpha} K_\gamma$ . In this case that  $K_\alpha$  is a local domain follows by transfinite induction. This proves the first part of the theorem. Now assume that  $\beta+1 < \alpha_0$ . Let  $x$  be the unique  $\inf^{(\beta+2)}$  prime and  $p$  the unique  $\inf^{(\beta+1)}$  prime in  $R$ . Then in  $K_\beta$   $p$  is the unique prime and  $x$  is the unique  $\inf^{(1)}$  prime. Hence  $K_\beta$  satisfies the hypotheses of Theorem 6 and so  $K_\beta$  is not a left Ore domain. From this it follows easily that  $R$  is not a left Ore domain. QED.

If  $R$  is a left Ore PRI domain such that  $R^* = R'$  then  $R$  is also a PLI domain. For each non-zero element of  $R$  has finite dimension. Consequently the restricted descending chain condition holds in  $R$  and therefore the ascending chain condition for principal left ideals holds in  $R$  (Lemma 2). Now  $R$  is a weak Bezout domain since  $R$  is a PRI domain. Since in addition  $R$  is a left Ore domain  $R$  is a left Bezout domain. In Chapter 1 we proved that right (left) Bezout domains satisfying the

ascending chain condition for principal right (left) ideals is a PRI (PLI) domain. Hence  $R$  is a PLI domain.

Corollary 1 Let  $R$  be a left Ore PRI domain. Let  $\beta_0$  denote the least ordinal in  $[0, \alpha_0]$  such that  $R_{\beta_0}$  is a local domain ( $R_{\alpha_0}$  is local since it is a field). Then either 1)  $\alpha_0 = 0$  and  $R$  is a PLI domain, or 2)  $\beta_0 = \alpha_0$ , or 3)  $\beta_0 + 1 = \alpha_0$ .

Proof. Assume the hypotheses. Suppose  $\alpha_0 \neq 0$  and  $\beta_0 \neq \alpha_0$ . Then by Theorem 7  $\beta_0 + 1 \neq \alpha_0$ . Hence  $\beta_0 + 1 \geq \alpha_0 > \beta_0$ . Therefore  $\beta_0 + 1 = \alpha_0$ . QED.

Corollary 2 A local left Ore PRI domain is a PLI domain.

Proof. Let  $R$  be a local left Ore PRI domain. If  $R$  is not a PLI domain then  $\alpha_0 \neq 0$ . Let  $\beta = -1$ . Then  $R_\beta = R$  is a local domain and  $\beta + 1 < \alpha_0$ . Hence by Theorem 7  $R$  is not a left Ore domain, a contradiction. QED.

The last two corollaries give conditions under which a PRI domain is also a PLI domain. We conjecture that Corollary 1 may be restated by omitting 3) from the conclusions. Indeed it may be true that every left Ore PRI domain is also a PLI domain. In particular no example is known to the author of a left Ore PRI domain that is not a PLI domain.

### 3.3 Example: skew polynomial extensions

We now introduce the important example of skew polynomial extensions which was defined by A. V. Jategaonkar in [8]. This example serves to illustrate some of the concepts that have been discussed. In particular we shall illustrate Theorem 5 for the local case.

If  $L$  is a ring and  $\sigma$  is a monomorphism from  $L$  into  $L$ , we shall denote by  $H = L[x, \sigma]$  the ring of skew polynomials in an indeterminate  $x$  with coefficients in  $L$  (written on the right of  $x$ ). Addition is the usual pointwise addition and multiplication is determined by the associative and distributive laws and by the commutation rule  $ax = x\sigma(a)$  ( $a \in L$ ). It is easy to prove that  $L$  is a subring of  $H$ , and if  $L$  is an integral domain, then so is  $H$  (see Ore [10]). Before proceeding with the example we shall need to establish two lemmas.

Lemma 22 Let  $H = L[x, \sigma]$ . Then  $H$  is a PRI domain iff  $L$  is a PRI domain and the non-zero members of  $L^\sigma$  are units of  $L$ .

Proof. See Jategaonkar [8].

Now if  $p$  is prime in  $L$  then clearly  $p$  is prime in  $H$ . It follows that if  $a \in L$  and  $a$  is a product of primes in  $L$  then  $a$  is a product of primes in  $H$ . Therefore if  $a \in L$  and  $\dim_L a < \infty$ , then  $\dim_H a < \infty$ .

Lemma 23 Let  $H = L[x, \sigma]$  be a PRI domain. If  $f \in H$  has a non-zero constant term  $a$  in  $L$  such that  $\dim_L a < \infty$ , then  $\dim_H f < \infty$ .

Proof. First we show that if  $d \in L$  and  $d \neq 0$  then  $1 + xd$  is prime in  $H$ . Suppose  $1 + xd = hg$ ,  $0 \neq d \in L$ ,  $h \in H$ , and  $g$  is a non-unit in  $H$ . If  $g \in L$  then  $g = c$  and  $h = a + xb$  where  $a, b, c \in L$ . Then  $1 + xd = ac + xbc$  which implies  $1 = ac$  and  $c$  is a unit, a contradiction. Therefore  $g \in H \setminus L$  and  $\deg g \geq 1$ . It follows that  $\deg g = 1$  and  $\deg h = 0$ .

Thus  $h = c$ ,  $g = a + xb$  ( $a, b, c \in L$ ). Then  $1 + xd = ca + cxb = ca + xc^\sigma b$ . Hence  $1 = ca$  and  $c$  is a unit. This shows that if  $1 + xd = hg$  and  $g$  is a non-unit then  $h$  is a unit. Consequently  $1 + xd$  is prime in  $H$ .

To prove the lemma we induct on  $\deg f$ . If  $\deg f = 0$ , then  $\dim_L f < \infty$  by hypothesis. It follows that  $\dim_H f < \infty$ . If  $\deg f = 1$ , then  $f$  is of the form  $f = a + xb = a(1 + x(a^\sigma)^{-1}b)$  where  $a, b \in L$ . Now  $\dim_L a < \infty$  by hypothesis and so  $\dim_H a < \infty$ . Since  $1 + x(a^\sigma)^{-1}b$  is prime, it has finite dimension. Consequently  $\dim_H f < \infty$ .

Let  $n > 1$  and assume the lemma holds for polynomials of degree less than  $n$ . Let  $f$  be a polynomial of degree  $n$  with finite dimensional constant term  $a_0$ . First assume  $a_0 = 1$ . If  $x$  is prime, then  $\dim_H f < \infty$ . If  $f$  is not prime then  $f = gh$  where  $g$  and  $h$  are non-units in  $H$ . If either  $g$  or  $h$  has degree zero then it must be a unit because  $a_0 = 1$ . Consequently  $0 < \deg g < n$ ,  $0 < \deg h < n$ . It follows by induction that  $g$  and  $h$  have finite dimension, and hence so does  $f$ . Now in the general case let  $f = a_0 + xa_1 + \dots + x^n a_n$  (where  $a_0$  need not equal 1). Then  $f = a_0(1 + x(a_0^\sigma)^{-1}a_1 + \dots + x^n(a_0^\sigma)^{-1}a_n)$  and hence  $f$  is the product of two elements of finite dimension. Therefore  $\dim_H f < \infty$ . QED.

We now turn our attention to the construction of the example of skew polynomial extensions. Let  $K$  be a (skew) field and let  $\bar{\alpha}$  be an ordinal. Let  $R$  be a right twisted polynomial extension of  $K$  with  $\{R_{(\alpha)} \mid \alpha \in [0, \bar{\alpha}]\}^1$  as a chain of twisted subdomains from  $K$  to  $R$  (see Jategaonkar [8]). Thus for each  $\alpha \in [0, \bar{\alpha}]^*$  there exists a monomorphism  $\rho_\alpha : R_{(\alpha-1)} \rightarrow R_{(\alpha-1)}$  and an indeterminate  $x_\alpha$  such that  $K = R_{(-1)}$  and such that the following conditions hold:

<sup>1</sup>This notation is not to be confused with  $K_\alpha = R(R^{(\alpha)})^{-1}$  which is still in force.

$$R_{(0)} = K[x_0, \rho_0] \text{ , } R = \bigcup_{\alpha \leq \bar{\alpha}} R_{(\alpha)} = R_{(\bar{\alpha})}$$

$$R_{(\alpha)} = R_{(\alpha-1)}[x_\alpha, \rho_\alpha] \text{ if } \alpha \in [0, \bar{\alpha}]^*$$

$$R_{(\alpha)} = \bigcup_{\beta < \alpha} R_{(\beta)} \text{ if } \alpha \in [0, \bar{\alpha}] \setminus [0, \bar{\alpha}]^*$$

Each element of  $R$  is a polynomial in a finite number of indeterminates  $x_\alpha$  with coefficients in  $K$ . We further require that  $(R_{(\alpha-1)})^{\rho_\alpha} \subset K$  for each  $\alpha \in [0, \bar{\alpha}]$  (Jategaonkar [8] shows how to construct such a system). Then  $R$  is a PRI domain by Lemma 22 and transfinite induction. In particular  $R$  has a right D-chain  $\{R^{(\alpha)} \mid 0 \leq \alpha \leq \alpha_0\}$ .

Lemma 24 Let  $S$  be the set of polynomials in  $R$  with non-zero constant terms. Then  $S \subset R^{(0)}$ , i.e., the members of  $S$  have finite dimension in  $R$ .

Proof. If  $g \in R^*$ , let  $l(g)$  denote the least ordinal  $\alpha$  such that  $g \in R_{(\alpha)}$ . Then  $l(g)$  is not a limit ordinal. To prove the lemma we use transfinite induction. If  $f \in S$  and  $l(f) = 0$  then  $f \in K[x_0, \rho_0]$ . Hence  $\dim f < \infty$  by Lemma 23, i.e.,  $f \in R^{(0)}$ . Let  $\alpha \in (0, \bar{\alpha}]^*$  and assume  $g \in S$ ,  $l(g) < \alpha$  implies  $g \in R^{(0)}$ . Let  $f \in S$  with  $l(f) = \alpha$ . Then  $f \in R_{(\alpha)} \setminus R_{(\alpha-1)}$ . It follows that  $f = h_0 + x_\alpha h_1 + \dots + x_\alpha^n h_n$  where  $h_i \in R_{(\alpha-1)}$  and  $h_0$  has a non-zero constant term in  $K$ . Let  $\beta = l(h_0)$ . Then  $\beta < \alpha$ . It follows by induction that  $\dim_{R_{(\beta)}} h_0 < \infty$ . Therefore  $\dim_{R_{(\alpha-1)}} h_0 < \infty$ . Lemma 23 applies and yields  $\dim_{R_{(\alpha-1)}} f < \infty$ . Hence  $\dim_R f < \infty$ , i.e.,  $f \in R^{(0)}$ . QED.

Lemma 25 For each  $\alpha \in [0, \bar{\alpha}]^*$ ,  $x_\alpha \in R \setminus R^{(\alpha-1)}$ .

Proof. The proof is by transfinite induction. Clearly  $x_0 \in R \setminus R^{(-1)}$  since  $x_0$  is not a unit in  $R$ . Let  $\alpha \in (0, \bar{\alpha}]^*$  and assume  $x_\beta \in R \setminus R^{(\beta-1)}$  whenever  $\beta \in [0, \alpha)^*$ . First assume  $\alpha-1$  is not a limit ordinal. Then  $x_\alpha = x_{\alpha-1} x_\alpha (x_{\alpha-1})^{\rho_{\alpha-1}-1} = (x_{\alpha-1})^2 x_\alpha (x_{\alpha-1})^{\rho_{\alpha-1}-2} = \dots$  which shows that

$x_\alpha \in \bigcap_{n=0}^{\infty} (x_{\alpha-1})^n R$ . Therefore  $x_\alpha \in \bigcap_{n=0}^{\infty} (x_{\alpha-1})^n K_{\alpha-2}$ . However  $x_{\alpha-1} \notin R^{(\alpha-1)}$  by induction and hence  $x_{\alpha-1}$  is a non-unit in  $K_{\alpha-2}$ . Consequently  $\dim_{K_{\alpha-2}} x_\alpha = \infty$ . This shows that  $x_\alpha \notin (K_{\alpha-2})^*$  and so  $x_\alpha \notin R^{(\alpha-1)}$ . On the other hand assume that  $\alpha-1$  is a limit ordinal. Let  $\delta$  be the least ordinal such that  $x_\alpha \in R^{(\delta)}$ . Then  $\delta$  is not a limit ordinal and so  $x_\alpha \in R^{(\delta)} \setminus R^{(\delta-1)}$ . If  $\delta < \alpha$  then since  $\delta \neq \alpha-1$ ,  $\delta < \alpha-1$ . Then the following equation  $x_\alpha = x_{\delta+1} x_\alpha (x_{\delta+1})^{-1} = (x_{\delta+1})^2 x_\alpha (x_{\delta+1})^{-2} = \dots$  shows that  $x_\alpha \in \bigcap_{n=0}^{\infty} (x_{\delta+1})^n R$ . Since  $\delta+1 < \alpha$  it follows by induction that  $x_{\delta+1} \notin R^{(\delta)}$  and therefore  $x_{\delta+1}$  is not a unit in  $K_\delta$ . Therefore  $x_\alpha \in \bigcap_{n=0}^{\infty} (x_{\delta+1})^n K_\delta$  and  $\dim_{K_\delta} x_\alpha = \infty$ . Hence  $x_\alpha \notin (K_\delta)^*$  and  $x_\alpha \notin R^{(\delta)}$ , contradicting the choice of  $\delta$ . It follows that  $\alpha \leq \delta$ . Therefore  $\alpha-1 \leq \delta-1$  and  $R \setminus R^{(\delta-1)} \subset R \setminus R^{(\alpha-1)}$ . Consequently  $x_\alpha \in R \setminus R^{(\alpha-1)}$ . QED.

We shall now show the relationship between  $R_{(\alpha)}$  and  $R^{(\alpha)}$ . As usual  $(R_{(\alpha)})^*$  denotes  $R_{(\alpha)} \setminus \{0\}$ .

Lemma 26 For each  $\alpha \in [0, \bar{\alpha}]$ ,  $(R_{(\alpha)})^* \subset R^{(\alpha)}$ .

Proof. The proof is by transfinite induction. Since  $R_{(0)} = K[x_0, \rho_0]$  each non-zero member of  $R_{(0)}$  is either a unit or is a product of primes (see Ore [10]). Hence if  $f \in R_{(0)}$  and  $f \neq 0$  then  $\dim_R f < \infty$  and so  $\dim_R f < \infty$ . Therefore  $R_{(0)} \subset R^{(0)}$ . Let  $\alpha \in (0, \bar{\alpha}]$  and assume that  $(R_{(\beta)})^* \subset R^{(\beta)}$  whenever  $\beta \in [0, \alpha)$ . If  $\alpha$  is a limit ordinal the proof is obvious. Assume that  $\alpha$  is not a limit ordinal. Let  $0 \neq f \in R_\alpha = R_{(\alpha-1)}[x_\alpha, \rho_\alpha]$ . Then  $f = x_\alpha^n h_n + \dots + x_\alpha^m h_m$  where  $h_i \in R_{(\alpha-1)}$  and  $h_n \neq 0$ . Then  $f = x_\alpha^n h_n (1 + x_\alpha (h_n)^{-1} h_{n+1} + \dots + x_\alpha^{m-n} (h_n^{m-n})^{-1} h_m)$ . The right factor has finite dimension by Lemma 24 and  $h_n \in R_{(\alpha-1)} \subset R^{(\alpha-1)}$  by induction. If we can show that  $x_\alpha$  is an  $\text{inf}^{(\alpha)}$  prime, then  $x_\alpha^n \in R^{(\alpha)}$  and therefore  $f \in R^{(\alpha)}$  which is the desired conclusion. Hence we proceed to show that  $x_\alpha$  is an  $\text{inf}^{(\alpha)}$  prime. Now  $x_\alpha \in R \setminus R^{(\alpha-1)}$  by Lemma 25. We claim that

$x_\alpha R$  is maximal in  $\{zR \mid z \in R \setminus R^{(\alpha-1)}\}$ . For suppose  $x_\alpha = kg$  where  $g$  is a non-unit in  $R$  and  $k \in R \setminus R^{(\alpha-1)}$ . Then by induction  $k \in R \setminus R_{(\alpha-1)}$ . Let  $\delta$  be the least ordinal such that  $k \in R_{(\delta)}$ . Then  $\delta$  is not a limit ordinal and  $\alpha \leq \delta$ . Since  $x_\alpha = kg$ , it must be a monomial in  $x_\delta$ :  $k = x_\delta b$ ,  $b \in R_{(\delta-1)}$ . If  $\delta = \alpha$ , then  $x_\alpha = kg = x_\alpha bg$  which implies  $1 = bg$  and  $g$  is a unit in  $R$ , a contradiction. If  $\alpha < \delta$ , then  $x_\delta = x_\alpha x_\delta (x_\alpha^\beta)^{-1}$ . Therefore  $x_\alpha = kg = x_\alpha x_\delta (x_\alpha^\beta)^{-1} bg$  which implies  $1 = x_\delta (x_\alpha^\beta)^{-1} bg$  and  $g$  is a unit, a contradiction. It follows that  $x_\alpha$  is an  $\text{inf}^{(\alpha)}$  prime. QED.

We have seen in the proof of Lemma 26 that  $x_\alpha$  is an  $\text{inf}^{(\alpha)}$  prime if  $\alpha \in [0, \bar{\alpha}]^*$ . In fact  $x_\alpha$  is the only (up to right unit factor)  $\text{inf}^{(\alpha)}$  prime if  $\alpha \neq 0$ . For if  $z$  is an  $\text{inf}^{(\alpha)}$  prime, then because  $\dim z = \infty$   $z$  has no non-zero constant term by Lemma 24. Hence  $z = ms$  where  $m$  is a monomial and  $s$  has a non-zero constant term. Since  $z$  is an  $\text{inf}^{(\alpha)}$  prime and since  $\dim s < \infty$  (by Lemma 24),  $s$  must be a unit (see Lemma 19). Hence we may assume that  $z$  has the form  $z = m = x_{\alpha_1} \dots x_{\alpha_k}$ . Since  $x_{\alpha_k}$  is a non-unit it follows (by the definition of  $\text{inf}^{(\alpha)}$  prime) that  $x_{\alpha_1} \dots x_{\alpha_{k-1}} \in R^{(\alpha-1)}$ . If  $\alpha_k < \alpha$ , then  $z \in R^{(\alpha-1)}$  which is impossible. If  $\alpha < \alpha_k$ , then  $x_{\alpha_k}$  is a prime and  $z$  is a unit in  $R_{\alpha_k-1}$ , and this is not possible. Therefore  $\alpha_k = \alpha$ . It follows that  $z = x_\alpha (x_{\alpha_1} \dots x_{\alpha_{k-1}})^k$ . The right factor is a unit and hence  $z$  and  $x_\alpha$  are right associates.

Next we note that  $\alpha_0 = \bar{\alpha}$ , for Lemma 26 shows that  $\bar{\alpha} \leq \alpha_0$ . Now  $R = R_{(\bar{\alpha})}$  so that  $R^* = (R_{(\bar{\alpha})})^* \subset R^{(\bar{\alpha})} \subset R^*$ . Therefore  $R = R^{(\bar{\alpha})}$ . It follows that  $R^{(\bar{\alpha})} = R^{(\bar{\alpha}+1)} = \dots$ . However  $\alpha_0$  is the least ordinal such that  $R^{(\alpha_0)} = R^{(\alpha_0+1)} = \dots$  by definition. Consequently  $\alpha_0 \leq \bar{\alpha}$  and hence  $\alpha_0 = \bar{\alpha}$ .

We are now able to state Theorem 5 for the present example as follows. The letter  $S$  denotes the set of polynomials of  $R$  with

non-zero constant terms (see Lemma 24).

Theorem 8 Each non-zero polynomial  $f \in R$  can be written as  $f = x_{\alpha_1}^{n_1} \dots x_{\alpha_k}^{n_k} s$  where  $n_i$  are positive integers,  $\alpha_1 > \dots > \alpha_k > 0$ , and  $s \in S$ . This expression is unique in the sense of Theorem 5. That is, if  $f = x_{\beta_1}^{m_1} \dots x_{\beta_h}^{m_h} r$  is another such factorization then  $h = k$ ,  $\alpha_i = \beta_i$  and  $n_i = m_i$  ( $i = 1, 2, \dots, k$ ), and there is a unit  $u \in R$  such that  $s = ur$ .



### 3.4 An example in the non-Bezout case

If  $R$  is not a right Bezout domain, we shall show by example that some of the desirable properties (e.g. Lemmas 20 and 21) need not hold. If  $R$  is an arbitrary integral domain we can define  $\dim a$  ( $a \in R^*$ ) to be the sup of the lengths of the chains in  $[aR, R]$  where  $[aR, R]$  is the set of principal right ideals of  $R$  that contain  $aR$ . However if  $R$  is not a right Bezout domain it seems unlikely that  $R' = \{a \in R \mid \dim a < \infty\}$  necessarily is a right quotient monoid (see Lemma 17). The construction of a D-chain employs the notion that if  $R'$  has the right quotient conditions and if  $K = R(R')^{-1}$ , then  $K'$  has the right quotient conditions. Therefore it would be difficult to extend this construction to non-Bezout domains. However we can still define infinite primes as usual. Let  $R$  be an integral domain and let  $S \subset R^*$  be a right quotient monoid in  $R$ . An element  $x \in R$  is called an S-prime iff  $xR$  is maximal in the set  $\{xR \mid x \in R \setminus S\}$ . We call  $R'$ -primes  $\inf^{(1)}$  primes as usual, and if  $R^{(\alpha)}$  exists for some non-limit ordinal  $\alpha$  as in Section 3.1 then we may speak of  $\inf^{(\alpha)}$  primes.

Let  $R$  be a local PRI domain with maximal ideal  $pR$  such that  $\{0\} \neq aR = \bigcap_{n=0}^{\infty} p^n R$  (for example we can let  $R$  be the domain described by Cohn in [5, p. 598] or we can construct  $R$  by taking  $\overline{\alpha} = 2$  in the last example and localizing). If  $x \in R$  then  $\dim x = \infty$  iff  $xR \subset \bigcap_{n=0}^{\infty} p^n R$ . Hence  $R \setminus R' = aR$ . Therefore  $a$  is the unique (up to right unit factor)  $\inf^{(1)}$  prime of  $R$ . Choose  $z \in R$  such that  $a = pz$ . Then  $\dim z = \infty$  and so  $z = at$  for some  $t \in R$ . Thus  $a = pat$ . Evidently  $t$  is a unit, otherwise  $aR \subsetneq paR$  contradicting the fact that  $a$  is an  $\inf^{(1)}$  prime. Now  $aR$  is an ideal since  $pR$  is an ideal. Thus  $Ra \subset aR$ . We define  $\sigma$  on  $R$

by  $ra = ar^\sigma$  for each  $r \in R$ . It is easy to check that  $\sigma$  is a monomorphism on  $R$ ,  $a^\sigma = a$ , and  $p^\sigma$  is a unit ( $p^\sigma = t^{-1}$ ).

Let  $K = R[[x, \sigma]]$  be the ring of skew formal power series in  $x$  with coefficients in  $R$  (written on the right of  $x$ ). Addition is pointwise and multiplication is determined by the associative and distributive laws and by the commutation rule  $rx = xr^\sigma$  ( $r \in R$ ) just as in the polynomial case. Then  $K$  is an integral domain with the property that each non-zero element in  $K$  is a unit iff it has a unit constant term in  $R$  (see Jategaonkar [7]).

Lemma 37 1)  $aK + xK = \bigcap_{n=0}^{\infty} p^n K$ , 2)  $aK \wedge xK = xaK = axK$ , and 3)  $aK + xK$  is not a principal right ideal.

Proof. Because  $a = pat = p^2 at^2 = \dots$  and  $x = pxt = p^2 xt^2 = \dots$ , it follows that  $a$  and  $x$  belong to  $\bigcap_{n=0}^{\infty} p^n K$  and therefore  $aK + xK \subset \bigcap_{n=0}^{\infty} p^n K$ . To prove the reverse inclusion suppose  $g \in \bigcap_{n=0}^{\infty} p^n K$ . We can write  $g$  in the form  $g = b + x\bar{g}$  where  $b \in R$ ,  $\bar{g} \in K$ . Then  $b = g - x\bar{g} \in \bigcap_{n=0}^{\infty} p^n K$ . Hence  $b \in \bigcap_{n=0}^{\infty} p^n R = aR$ . Consequently  $g \in aK + xK$ . Thus 1) is established. Now  $ax = xa$  because  $a^\sigma = a$ . Therefore  $xa \in xK \wedge aK$  and  $xaK \subset xK \wedge aK$ . If  $xf = ag \in xK \wedge aK$  then clearly  $g$  cannot have a constant term, so that  $g = x\bar{g}$  for some  $\bar{g} \in K$ . Therefore  $xf = ag = ax\bar{g} = xag \in xaK$ . Thus  $xK \wedge aK \subset xaK$  and 2) is established. To prove 3) suppose there exists  $d \in K$  such that  $aK + xK = dK$ . Then  $a = dg$  for some  $g \in K$ . Obviously both  $d$  and  $g$  belong to  $R$  because  $a$  belongs to  $R$ . We claim that  $d \in R \setminus aR$ , for if  $d \in aR$ , then since  $x \in dK$  it follows that  $x \in aK$ . Let  $f \in K$  such that  $x = af$ . Clearly  $f$  must be a monomial, say,  $f = xb$  ( $b \in R$ ). Then  $x = axb = xab$ ,  $1 = ab$ , and  $a$  is a unit. This contradiction shows that  $d \in R \setminus aR$ . It follows that  $d = p^n u$  where  $u$  is a unit in  $R$ . Consequently

$xK + aK = p^n K$  contradicting part 1). It follows that  $xK + aK$  is not a principal right ideal. QED.

Lemma 28 Let  $f \in K^*$ . Then  $\dim_K f < \infty$  iff  $f$  has a non-zero constant term  $b$  such that  $\dim_R b < \infty$ .

Proof. Assume  $\dim_K f < \infty$ . Let  $f = b + xf$  ( $b \in R$ ,  $\bar{f} \in K$ ). Then since  $\dim_K x = \infty$  it follows that  $b \neq 0$ . If  $b \in aR$  then  $f \in aK + xK = \bigcap_{n=0}^{\infty} p^n K$  and this implies that  $\dim_K f = \infty$ , a contradiction. Hence  $b \in R \setminus aR$  and therefore  $\dim_R b < \infty$ . Conversely assume  $f$  has a non-zero constant term  $b$  such that  $\dim_R b < \infty$ . Then  $b \in R \setminus aR$  so that  $b = p^n u$  where  $u$  is some unit in  $R$ . Then  $f = p^n u + xf = p^n u(1 + u^{-1}x((p^n)^{\sigma})^{-1}\bar{f})$ ; the left factor has finite dimension and the right factor is a unit in  $K$ . Therefore  $\dim_K f < \infty$ . QED.

Lemma 28 and the first part of Lemma 27 together yield the following.

Corollary  $K \setminus K' = aK + xK$ .

Lemma 29 The set  $K'$  is a right quotient monoid.

Proof. Clearly  $0 \notin K'$ ,  $1 \in K'$  and  $fg \in K'$  iff  $f, g \in K'$ . Let  $f \in K$  and  $g \in K'$ . We must find  $\bar{f} \in K$ ,  $\bar{g} \in K'$  such that  $f\bar{g} = g\bar{f}$ . We consider two cases.

Case 1: Assume  $g \in R$ . Let  $f = b_0 + xb_1 + \dots$ . Since  $\dim_R g < \infty$ , it follows that  $g^{\sigma}$  is a unit in  $R$ . Choose  $\bar{b}_0, \bar{g} \in R$  with  $\dim_R \bar{g} < \infty$  such that  $b_0\bar{g} = g\bar{b}_0$  (this is possible because  $R'$  is a right quotient monoid in  $R$ ). Let  $\bar{b}_i = (g^{\sigma})^{-1}b_i\bar{g}$  ( $i = 1, 2, \dots$ ), and let  $\bar{f} = \bar{b}_0 + x\bar{b}_1 + \dots$ . Then  $f\bar{g} = g\bar{f}$  and  $\bar{g} \in K'$ .

Case 2: Let  $g$  be arbitrary in  $K'$ . Then  $g = p^n u + xg'$  where  $u$  is a unit in  $R$  and  $g' \in K$  (by Lemma 28). Let  $h = 1 + u^{-1}x((p^n)^{\sigma})^{-1}g'$ .

Then  $g = p^n uh$  and  $h$  is a unit in  $K$ . By case 1 we can find  $f' \in K$  and  $\bar{g} \in K'$  such that  $f\bar{g} = (p^n u)f'$ . Let  $\bar{f} = h^{-1}f'$ . Then  $f\bar{g} = g\bar{f}$ .  $\square$

Because  $a$  is an  $\text{inf}^{(1)}$  prime in  $R$  it follows that  $a$  is an  $\text{inf}^{(1)}$  prime in  $K$ . A simple argument shows that  $x$  is an  $\text{inf}^{(1)}$  prime in  $K$ . Also it follows by the corollary to Lemma 28, Lemma 29, and Lemma 10 that  $L = K(K')^{-1}$  is a local domain. Thus Lemmas 20 and 21 do not hold for the present example.

## CHAPTER IV

## APPLICATION TO FINITE DIMENSIONAL ELEMENTS IN A RIGHT BEZOUT DOMAIN

4.1 Unique factorization and similar primes

In this section we use the Factorization lemma to obtain some results concerning prime factorization in a right Bezout domain  $R$ . For this purpose we shall proceed to construct another collection of right quotient monoids in  $R$ .

Let  $P$  be a set of primes in  $R$  such that each prime in  $R$  is similar to one and only one member of  $P$ . For an arbitrary subset  $A$  of  $P$  we consider the set  $S_A$  of finite dimensional elements  $z$  of  $R$  such that  $z$  has no prime factor that is similar to any member of  $A$ .

Lemma 30 Let  $R$  be a right Bezout domain. Let  $A \subset P$  where  $A$  and  $P$  are the sets described in the last paragraph. Then  $S_A$  is a right quotient monoid.

Proof. Clearly  $0 \notin S_A$  and  $1 \in S_A$ . Now  $a \in S_A$ ,  $\bar{a} \in R$ ,  $a \sim \bar{a}$  implies  $\bar{a} \in S_A$  follows from Theorem 2. It is also true that  $ab \in S_A$  iff  $a, b \in S_A$ . It then follows from the second part of Lemma 7 that  $S_A$  is a right quotient monoid. QED.

If  $A = P \setminus \{p\}$  where  $p \in P$ , we shall denote  $S_A$  by  $S_p'$ , and if  $A = \{p\}$ , then we shall denote  $S_A$  by  $S_p$ . We note that if  $p$  is a prime in a right Bezout domain  $R$  then  $K = R(S_p)^{-1}$  is a right Bezout domain with the property that all primes of  $K$  are similar to  $p$ .

Definition An element  $a$  in an integral domain  $R$  is called p-primary if  $a$  is the product of primes that are similar to  $p$  where  $p$  is a prime in  $R$ .

In a right Bezout domain  $R$  the set  $S_p^{-1}$  is just the set of elements of  $R$  that are either  $p$ -primary or units. Now it is obvious that each element  $z$  in  $R'$  is the product of  $p_i$ -primary elements where  $p_i$  are the primes that occur in a factorization of  $z$ . With an additional hypothesis we are able to establish uniqueness of this primary factorization in two different respects.

Theorem 9 Let  $R$  be a right Bezout domain. Let  $z = a_{p_1} \dots a_{p_n}$  be a factorization of  $z$  into  $p_i$ -primary elements  $a_{p_i}$  with  $p_i \not\sim p_j$  whenever  $i \neq j$ . Then the factorization of  $z$  is unique in the sense that if  $z = b_{p_1} \dots b_{p_n}$  is another such factorization of  $z$  then there are units  $u_1, \dots, u_{n-1}$  in  $R$  such that  $a_{p_1} = b_{p_1} u_1$ ,  $a_{p_n} = u_{n-1}^{-1} b_{p_n}$ , and  $a_{p_i} = u_{i-1}^{-1} b_{p_i} u_i$  ( $i \neq 1, n$ ).

Proof. Let  $z = a_{p_1} \dots a_{p_n} = b_{p_1} \dots b_{p_n}$  be two primary factorizations of  $z$  such that  $p_i \not\sim p_j$  if  $i \neq j$ . Let  $x_1 = a_{p_1} \dots a_{p_{n-1}}$ ,  $s_1 = a_{p_n}$ ,  $x_2 = b_{p_1} \dots b_{p_{n-1}}$ ,  $s_2 = b_{p_n}$  and  $S = S_{p_n}^{-1}$ . Then the hypotheses of the second part of the Factorization lemma are satisfied and hence  $x_1 = x_2 u$  for some unit  $u \in R$ . Theorem 9 now follows by induction. QED.

Before stating the next theorem we note that if  $R$  is a weak Bezout domain and  $z \in R'$  then the number of primes that are (pairwise) dissimilar in a prime factorization of  $z$  is invariant in any prime factorization of  $z$  (see Theorem 1).

Theorem 10 Let  $R$  be a right Bezout domain. If  $z$  is a non-unit in  $R'$  and  $z = a_{p_1} \dots a_{p_n} = b_{q_1} \dots b_{q_m}$  are two primary factorizations of  $z$  such that  $a_{p_i}$  is  $p_i$ -primary,  $b_{q_i}$  is  $q_i$ -primary,  $p_i \not\sim p_j$  if  $i \neq j$ , and  $q_i \not\sim q_j$  if  $i \neq j$  then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  such that  $a_{p_i} \sim b_{q_{\pi(i)}}$  ( $i = 1, 2, \dots, n$ ).

Proof. Suppose  $a_{p_1} \dots a_{p_n} = b_{q_1} \dots b_{q_m}$  as in the hypotheses. That  $n = m$  follows from the preceding remarks. To prove uniqueness up to similarity we induct on  $n$ . If  $n = 1$  there is nothing to prove. If  $n = 2$  then  $a_{p_1} a_{p_2} = b_{q_1} b_{q_2}$ . If  $p_1 \sim q_1$  then  $a_{p_1} = b_{q_1} u$  for some unit  $u \in R$  by the Factorization lemma (let  $B$  be the subset of  $P$  consisting of those and only those primes that are similar to some member of  $\{p_2, q_2\}$ , let  $A = P \setminus B$ ,  $S = S_A$ ,  $x_1 = a_{p_1}$ ,  $x_2 = b_{q_1}$ ,  $s_1 = a_{p_2}$ ,  $s_2 = b_{q_2}$ , and apply the second part of the Factorization lemma). If  $p_1 \not\sim q_1$  then  $a_{p_1} R + b_{q_1} R = R$  (otherwise  $a_{p_1}$  and  $b_{q_1}$  would have a common prime factor). Let  $n \in R$  such that  $a_{p_1} R \cap b_{q_1} R = nR$ ,  $a_{p_1} \bar{b} = b_{q_1} \bar{a} = m$ . Thus  $a_{p_1} \sim \bar{a}$ ,  $b_{q_1} \sim \bar{b}$ . Now  $a_{p_1} a_{p_2} \in mR$  so that  $a_{p_1} a_{p_2} = b_{q_1} b_{q_2} = a_{p_1} \bar{b} r = b_{q_1} \bar{a} r$  for some  $r \in R$ . Hence  $a_{p_2} = \bar{b} r$  and  $b_{q_2} = \bar{a} r$ . If  $r$  has a prime factor then that prime factor must be similar to both  $p_2$  and  $q_2$ , i.e.,  $p_2 \sim q_2$  and hence  $p_1 \sim q_1$ , a contradiction. Hence  $r$  is a unit. It follows that  $a_{p_1} \sim b_{q_1}$  and  $b_{q_2} \sim a_{p_2}$ .

Let  $z = a_{p_1} \dots a_{p_n} = b_{q_1} \dots b_{q_n}$  with  $n \geq 3$  and assume that the theorem holds for integers less than  $n$ . If  $p_1 \sim q_1$  then again we find  $a_{p_1} = b_{q_1} u$  for some unit  $u \in R$  by the Factorization lemma. (let  $B$  be the subset of  $P$  consisting of those and only those primes that are similar to some member of  $\{p_2, \dots, p_n, q_2, \dots, q_n\}$ , let  $A = P \setminus B$ ,  $S = S_A$ ,  $x_1 = a_{p_1}$ ,  $x_2 = b_{q_1}$ ,  $s_1 = a_{p_2} \dots a_{p_n}$ ,  $s_2 = b_{q_2} \dots b_{q_n}$ ). Hence  $a_{p_2} \dots a_{p_n} = u^{-1} b_{q_2} \dots b_{q_n}$  and the theorem follows by induction. If  $p_1 \not\sim q_1$  then  $p_1 \sim q_k$  where  $k > 1$ . Then for each  $i \leq k-1$ ,  $a_{p_1} R + b_{q_1} \dots b_{q_i} R = R$ , and  $a_{p_1} R \cap b_{q_1} \dots b_{q_i} R = m_i R$  where  $m_i = a_{p_1} b_i = b_{q_1} \dots b_{q_i} a_i$  for some  $b_i, a_i \in R$ . Hence  $a_{p_1} \sim a_i$ . Now  $z \in m_i R$  so  $z = a_{p_1} b_i r_i = b_{q_1} \dots b_{q_i} a_i r_i$  for some  $r_i \in R$ . Hence  $b_{q_{i+1}} \dots b_{q_n} = a_i r_i$ . In particular  $b_{q_k} \dots b_{q_n} = a_{k-1} r_{k-1}$ . Since  $a_{k-1} \sim a_{p_1}$  the prime factors of  $a_{k-1}$  are similar to  $p_1$  and since  $p_1 \sim q_k$  the prime factors of  $b_{q_k}$  are similar to  $p_1$ . If  $k = n$  then  $r_{k-1}$

is a unit. If  $k < n$ , let  $B$  be the subset of  $P$  consisting of those and only those primes that are similar to some member of  $\{q_{k+1}, \dots, q_n\}$ , let  $A = P \setminus B$ ,  $S = S_A$ ,  $x_1 = b_{q_k}$ ,  $x_2 = a_{k-1}$ ,  $s_1 = b_{q_{k+1}} \dots b_{q_n}$ ,  $s_2 = r_{k-1}$ . Then by the second part of the Factorization lemma we obtain a unit  $u \in R$

such that  $b_{q_k} = a_{k-1}u$ . Hence in either case  $b_{q_k} = a_{k-1}u$  for some unit  $u$  and  $ub_{q_{k+1}} \dots b_{q_n} = r_{k-1}$  ( $u = r_{k-1}$  if  $k = n$ ). Also  $a_{p_1} \sim b_{q_k}$  since  $a_{p_1} \sim a_{k-1}$ .

Now  $m_1 R \supset \dots \supset m_{k-1} R$  and so  $m_{i+1} = m_i \bar{m}_i$  for some  $\bar{m}_i \in R$ . Then

$a_{p_1} b_{i+1} = m_{i+1} = m_i \bar{m}_i = a_{p_1} b_i \bar{m}_i$  and hence  $b_{i+1} = b_i \bar{m}_i$ . Hence

$b_{k-1} = b_1 \bar{m}_1 \dots \bar{m}_{k-2}$  ( $b_{k-1} = b_1$  if  $k = 2$ ). From  $m_{i+1} = m_i \bar{m}_i$  we also obtain

$b_{q_1} \dots b_{q_{i+1}} a_{i+1} = m_{i+1} = m_i \bar{m}_i = b_{q_1} \dots b_{q_i} a_i \bar{m}_i$ . Thus  $b_{q_{i+1}} a_{i+1} = a_i \bar{m}_i$ .

Since  $a_{i+1} \sim a_{p_1} \sim a_i$  it follows by induction that  $b_{q_{i+1}} \sim \bar{m}_i$ . Since

$z = a_{p_1} \dots a_{p_n} = a_{p_1} b_{k-1} r_{k-1}$ ,  $b_{k-1} = b_1 \bar{m}_1 \dots \bar{m}_{k-2}$ , and  $r_{k-1} = ub_{q_{k+1}} \dots b_{q_n}$

we obtain  $a_{p_2} \dots a_{p_n} = b_1 \bar{m}_1 \dots \bar{m}_{k-2} ub_{q_{k+1}} \dots b_{q_n}$  ( $a_{p_2} \dots a_{p_n} = b_1 \bar{m}_1 \dots \bar{m}_{k-2} u$

if  $k = n$ ). It follows by induction that the members of the two sets

$\{a_{p_2}, \dots, a_{p_n}\}$  and  $\{b_1, \bar{m}_1, \dots, \bar{m}_{k-2}, (ub_{q_{k+1}}), \dots, b_{q_n}\}$

( $\{b_1, \bar{m}_1, \dots, \bar{m}_{k-2} u\}$  if  $k = n$ ) may be paired into similar pairs. Since

$b_1 \sim b_{q_1}$  and  $\bar{m}_1 \sim b_{q_{i+1}}$  the members of the sets  $\{a_{p_2}, \dots, a_{p_n}\}$  and

$\{b_{q_1}, \dots, b_{q_{k-1}}, b_{q_{k+1}}, \dots, b_{q_n}\}$  ( $\{b_{q_1}, \dots, b_{q_{k-1}}\}$  if  $k = n$ ) may be

paired into similar pairs. QED.



## 4.2 Example

If  $R$  is a commutative right Bezout domain the hypothesis in Theorem 9 is trivially satisfied. However in general this hypothesis need not hold. It is also true that the number of primary factors in primary decompositions of an element may vary. The following example which is considered by Johnson in [3] illustrates such phenomena.

Before proceeding we shall need a lemma. If  $p_1, \dots, p_n$  are primes, then  $z = p_1 \dots p_n$  is called a rigid factorization of  $z$  and  $z$  is called rigid if the only other prime factorizations of  $z$  have the form  $z = (p_1 u_1)(u_1^{-1} p_2 u_2) \dots (u_{n-1}^{-1} p_n)$  where  $u_1, \dots, u_{n-1}$  are units in  $R$  (this terminology is used by Cohn in [3] and [4]).

**Lemma 32** Let  $R$  be a weak Bezout domain. Let  $p$  and  $q$  be primes in  $R$  such that  $pq, qp, p^2, q^2$  are rigid. If  $n > 0$  and  $r_i \in \{p, q\}$  ( $i = 1, 2, \dots, n$ ), then  $z = r_1 \dots r_n$  is rigid.

**Proof.** The proof is by induction. If  $n = 1$  or  $n = 2$  there is nothing to prove. Assume  $n \geq 3$  and let  $z = r_1 \dots r_n = s_1 \dots s_n$  where  $s_i$  are arbitrary primes and  $r_i \in \{p, q\}$ . Since  $R$  is a weak Bezout domain we may choose  $d, m, \bar{r}_1, \bar{s}_1 \in R$  such that  $r_1 R + s_1 R = dR$ ,  $r_1 R \wedge s_1 R = mR$ , and  $m = r_1 \bar{s}_1 = s_1 \bar{r}_1$ . If  $r_1 R = s_1 R$  then  $r_1$  and  $s_1$  are right associates. Cancelling these factors in  $z$  the lemma follows by induction. Hence we assume that  $r_1 R \neq s_1 R$ . Then  $r_1 R \not\subseteq dR$  and so  $dR = R$  since  $r_1$  is prime. Hence  $s_1 \sim \bar{s}_1$  and therefore  $\bar{s}_1$  is prime. Now  $z \in r_1 R \wedge s_1 R$  implies that  $r_1 \dots r_n = r_1 \bar{s}_1 x$  and hence  $r_2 \dots r_n = \bar{s}_1 x$  for some  $x \in R$ . Applying induction we obtain  $r_2 = \bar{s}_1 u$  for some unit  $u \in R$ . From  $r_1 \bar{s}_1 = s_1 \bar{r}_1$  we obtain  $r_1 r_2 = s_1 \bar{r}_1 u$ . Again by induction there is a unit  $v \in R$  such that  $r_1 = s_1 v$ . Therefore  $r_1 R = s_1 R$ , a contradiction. QED.

Let  $R = F[x, \sigma]$  be the ring of skew polynomials described earlier

in Chapter 1, where  $F = \mathbb{Z}_2(t)$  is a transcendental extension of  $\mathbb{Z}_2$ , the ring of integers modulo 2. We take  $\sigma$  to be the endomorphism on  $F$  defined by  $a^\sigma = a^2$ . Thus  $R$  is a PRI domain (but not a PLI domain) with multiplication determined by the formula  $ax = xa^2$  ( $a \in F$ ).

It is obvious that if  $a \in F$  then  $a + x$  is prime in  $R$ . Further the equation  $(a + x)(b^2a^{-2}) = ba^{-1}(b + x)$  shows that  $a + x \sim b + x$  if  $a$  and  $b$  are both non-zero. Conversely if  $0 \neq a \in F$ , then  $a + x \not\sim x$ , for otherwise  $xR + fR = R$ ,  $xR \cap fR = f(x + a)R$ , and  $f(x + a) = xg$  for some  $f, g \in R$ . Now since  $xR + fR = R$ ,  $f$  must have a constant term unequal to zero. Therefore from  $f(x + a) = xg$  we must obtain  $g = 0$ . Hence  $f = 0$ , a contradiction.

It is also interesting to note that in any polynomial domain  $R$  over a field  $F$ , if  $f \sim g$ , then  $\deg f = \deg g$ . For  $f \sim g$  implies  $R/fR \cong R/gR$  as  $R$ -modules and therefore also as  $F$ -modules. Hence  $R/fR$  and  $R/gR$  must have the same vector space dimension over  $F$ . Evidently the dimension of  $R/fR$  over  $F$  is the degree of  $f$  because if  $f = x^n + x^{n-1}a_{n-1} + \dots + a_0$  (without loss in generality we assume that  $f$  is monic) then  $\{x^{n-1}, \dots, x, 1\}$  is a basis for  $R/fR$  over  $F$ . Similar remarks apply for  $g$  and therefore  $\deg f = \deg g$ .

It has already been noted that  $1 + x$  is prime and it can be verified that  $t + x^2$  is prime. We shall now show that these two primes satisfy the hypotheses of Lemma 32.

**Lemma 33** In  $R = (\mathbb{Z}_2(t))[x, \sigma]$  the following elements are rigid:  $(1 + x)(t + x^2)$ ,  $(t + x^2)(1 + x)$ ,  $(1 + x)^2$ , and  $(t + x^2)^2$ .

**Proof.** To show that  $(1 + x)(t + x^2)$  is rigid suppose that  $(1 + x)(t + x^2) = pq$  where  $p$  and  $q$  are primes in  $R$ . Clearly we may

assume that  $p$  and  $q$  are monic polynomials. By Theorem 1  $p$  is similar to one of  $(1 + x)$ ,  $(t + x^2)$  and  $q$  is similar to the other. Therefore there are two cases.

Case 1:  $\deg p = 2$  and  $\deg q = 1$ . Then  $p = d + xc + x^2$  and  $q = a + x$  for some  $a, c, d \in F$ . Expanding  $(1 + x)(t + x^2) = (d + xc + x^2)(a + x)$  and equating corresponding coefficients we obtain  $t = da$ ,  $t = ca + d^2$ , and  $1 = a + c^2$  which yield  $t^2(a^4 + t^2) = a^6(1 + a)$ . Let  $a = f/g$  where  $f$  and  $g$  are relatively prime polynomials in  $\mathbb{Z}_2[t]$ . Then by substituting in the last equation we obtain  $t^4g^7 = f^4(t^2g^3 + f^3 + f^2g)$ . Therefore  $t^4$  must divide the right side of the last equation. Because  $f$  and  $g$  are relatively prime it follows that  $t/f$ , say,  $f = tf'$ . Then  $g^7 = t^2f'^4(g^3 + tf'^3 + f'^2g)$ , and so  $t/g$ , a contradiction. That is, Case 1 is not possible.

Case 2:  $\deg q = 2$  and  $\deg p = 1$ . Then  $p = a + x$  and  $q = d + xc + x^2$  for some  $a, c, d \in F$ . Expanding the equation  $(1 + x)(t + x^2) = (a + x)(d + xc + x^2)$  and equating corresponding coefficients we obtain  $t = ad$ ,  $t = d + a^2c$ , and  $1 = a^4 + c$  which yield  $t(1 + a) = a^3(1 + a)^4$ . If  $1 + a \neq 0$  then  $t = (a(1 + a))^3$ , and this is not possible. Therefore  $1 + a = 0$ , i.e.,  $a = 1$ . It follows that  $d = t$  and  $c = 0$ . Hence  $p = 1 + x$  and  $q = t + x^2$ .

Similar arguments are used to prove that  $(t + x^2)(1 + x)$ ,  $(t + x^2)^2$ , and  $(1 + x)^2$  are rigid. QED.

Combining Lemmas 32 and 33 it follows that any product whose factors belong to  $\{(1 + x), (t + x^2)\}$  is rigid. In particular  $z = (1 + x)(t + x^2)(1 + x)$  is rigid. Also  $(1 + x)$  and  $(t + x^2)$  are not similar because they have different degrees. Hence  $z$  cannot be given a primary factorization of the type described in the hypothesis of

Theorem 9. Finally we note that the number of primary factors in primary factorizations of a given element is not necessarily a constant. For if  $0 \neq a \in F$  then the equation  $x(a+x)x = x^2(a^2+x)$  contains three primary factors on the left side and two primary factors on the right side.

## BIBLIOGRAPHY

1. G. Birkhoff, Lattice Theory, Am. Math. Soc. Colloquim Publication, Vol. 25, 1967.
2. N. Bourbaki, Elements de mathematique; Algebre commutative, chapitre 2, Hermann, Paris, 1961.
3. P. M. Cohn, Noncommutative unique factorization domains, Trans. Am. Math. Soc., 109 (1963), 313-331.
4. P. M. Cohn, Hereditary local rings, Nagoya Math. J., 27 (1966), 223-230.
5. P. M. Cohn, Torsion modules over free ideal rings, London Math. Soc., 17 (1967), 557-599.
6. N. Jacobson, Theory of rings, Am. Math. Soc., Providence, R. I., 1943.
7. A. V. Jategaonkar, Left principal ideal domains, J. of Algebra, 8 (1968), 146-155.
8. A. V. Jategaonkar, A counter example in ring theory and homological algebra, To appear.
9. R. B. Johnson, Unique factorization in a principal right ideal domain, Proc. Am. Math. Soc., 16 (1965), 526-528.
10. O. Ore, Theory of noncommutative polynomials, Ann. of Math., 34 (1933), 480-508.
11. O. Zariski and P. Samuel, Commutative Algebra, Vol. 1, Van Nostrand Co., New York, N. Y.